(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年9 月1 日 (01.09.2005)

PCT

(10) 国際公開番号
WO 2005/081460 A1

(51) 国際特許分類[7]: H04L 12/28, H04Q 7/38

(21) 国際出願番号: PCT/JP2005/002494

(22) 国際出願日: 2005 年2 月17 日 (17.02.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-042303 2004 年2 月19 日 (19.02.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 丹生 隆之 (NYU, Takayuki) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP).

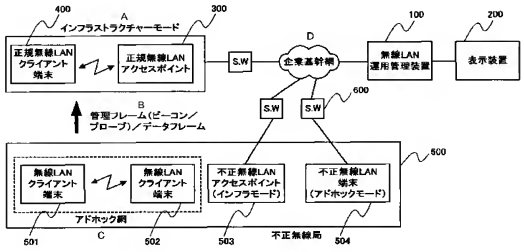
(74) 代理人: 宇高 克己 (UDAKA, Katsuki); 〒1010025 東京都千代田区神田佐久間町１－１４第二東ビル５階 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA,

[続葉有]

(54) Title: UNAUTHORIZED WIRELESS STATION DETECTING SYSTEM, APPARATUS USED THEREIN, AND METHOD THEREFOR

(54) 発明の名称: 不正無線局検出システム、それに用いる装置及びその方法



A .. INFRASTRUCTURE MODE
400 .. AUTHORIZED WIRELESS LAN CLIENT TERMINAL
300... AUTHORIZED WIRELESS LAN ACCESS POINT
D... INTRACORPORATE TRUNK NETWORK
100... WIRELESS LAN OPERATIONAL MANAGEMENT APPARATUS
200... DISPLAY DEVICE
B... MANAGEMENT FRAMES (BEACON/PROBE)/DATA FRAMES
500... UNAUTHORIZED WIRELESS STATION
C... AD HOC NETWORK
501 .. WIRELESS LAN CLIENT TERMINAL
502... WIRELESS LAN CLIENT TERMINAL
503 .. UNAUTHORIZED WIRELESS LAN ACCESS POINT (INFRA MODE)
504... UNAUTHORIZED WIRELESS LAN TERMINAL (AD HOC MODE)

(57) Abstract: Wireless stations (300,400) to be managed search the wireless space over a plurality of frequency channels to acquire, from frames propagating in the space, BSS identifiers and frame transmitting source identifiers that are unique IDs. An operational management apparatus (100) receives those acquired BSS identifiers and frame transmitting source identifiers, and compares them with registered BSS identifiers to detect an unauthorized wireless station (500) and further determine the type and manufacturer thereof. Moreover, the operational management apparatus (100) notifies the wireless stations to be managed, namely, an authorized base station (300), an authorized terminal (400), a switch apparatus (600) and so on of the existence of the unauthorized wireless station, and then instructs abandonment of frames from the unauthorized wireless station (500), disconnection of communication therefrom or the like so as to take measures of disabling communication with the unauthorized wireless station.

(57) 要約: 管理対象の無線局３００，４００は、複数の周波数チャネルにわたり無線空間を検索し、空間を伝搬しているフレームから固有ＩＤであるＢＳＳ識別子とフレーム送信元識別子とを取得する。運用管理装置１００はこれら取得されたＢＳＳ識別子とフレーム送信元識別子を得て、登録されたＢＳＳ識別子と比較し不正無線局５００を検出すると共に、その種別や製造元をも判定する。更に、運用管理装置１００は、この不正無線局の存在を管理対象無線局すなわち正規基地局３００、正規端末４００、スイッチ装置６００などへ通知し、不正無線局５００からのフレーム破

[続葉有]

WO 2005/081460 A1

NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

不正無線局検出システム、それに用いる装置及びその方法

技術分野

[0001] 本発明は不正無線局検出システム及びそれに用いる運用管理装置、無線基地局、無線通信端末並びにその方法に関し、特に無線LANシステムを利用する環境において出現する無線局の監視及び該無線局からの情報漏洩の防止方法に関するものである。

背景技術

[0002] 無線LANシステムにおいて、不正アクセスポイント(AP)の検出に関しては、特許文献1において、ネットワークセキュリティシステム、コンピュータ装置、アクセスポイントの認識処理方法、アクセスポイントのチェック方法、プログラム、記憶媒体及び無線LAN用デバイスに関する技術が開示されている。

[0003] 開示された発明の説明の前に、識別子として使用されているSSIDについて説明する。無線LAN(IEEE802.11)では、互いに通信する端末、基地局のグループを基本サービスセット(Basic Service Set)と呼び、そのグループの識別子をBSSIDと呼ぶ。基地局と端末が通信するモードでは基地局の物理アドレス(MAC(Media Access Control)アドレス)が使用される。端末同士が通信するモード(アドホックモード)では端末が割り振る任意の値(各端末で割り振るため厳密には一意性は保証されない)である。また、1つ以上のBSSから構成されるグループ(無線LANシステム)を拡張サービスセット(ESS)と呼び、このグループの識別子をSSIDと呼ぶ。

[0004] 開示された発明においては、図1の無線LANシステムにおいて、正規(管理対象)無線LANクライアントがスキャン処理を実行することにより、周囲のアクセスポイント(以下AP)のパケットから無線LANの識別子(SSID:Service Set ID)を抽出し、SSIDから構成されるAP検出リストを作成する。次に、予め登録されたAP許可リストと比較して、登録されていないSSIDが存在した場合には、不正なAPが存在すると判断され、不正APが存在する位置を通知することにより、その不正なAPを撤去することが可能になる。また、不正APを検出した場合にルータを操作して不正APとのデータの

送受信を禁止する。

特許文献1:特開2003−198571号公報

発明の開示

発明が解決しようとする課題

[0005] しかしながら、開示されている発明には以下の課題がある。第一の課題は、不正APの識別子として一意ではない無線LANシステムの識別子を用いていることである。具体的には、無線LANシステムの識別子(SSID:Service Set ID)は、無線LANシステム構築時に設定される識別子であり、ユーザが容易に変更可能な値であるため、SSIDを登録済みSSIDと詐称する不正なAPは検出できないという問題がある。

[0006] また、前述の通り、無線LAN基地局(AP)に対して、同一の無線LANシステムの識別子(SSID)が割当可能であるため、SSIDを用いて不正APの探査を行うと、不正なAPの数が単一であるか複数であるかを識別することができず、撤去作業を行う管理者が探査・撤去する不正APの数を判断できないという問題がある。

[0007] 第二の課題は、無線LANシステムの識別子(SSID)のみで不正APを検出していることである。具体的には、無線LANシステムの識別子(SSID)を出力する機器は、インフラストラクチャモードで動作する無線LAN基地局(AP)、アドホックモードで動作する無線LANクライアントがあるが、開示された発明では、これらを区別していないため無線LAN基地局(AP)と無線LANクライアントの両方を不正無線局の候補として探査する必要があり、探査効率が悪いという問題がある。

[0008] 第三の課題は、SSIDの秘匿機能を備えた無線LAN機器が市場に存在するため、不正な基地局(AP)がその機能を利用している場合にそれを検出できないことである。第四の課題は、不正な基地局(AP)とのデータの送受信を禁止する具体的な記載がないことである。

[0009] 本発明は上記課題を解決するためになされたものであって、不正無線局の存在を検出・通知し、該不正無線局からの情報漏洩を防止することによるセキュリティの向上と、当該セキュリティ管理作業の効率化とを実現する不正無線局検出システム及びそれに用いる運用管理装置、無線基地局、無線通信端末並びにその方法を提供することである。

課題を解決するための手段

[0010] 上記課題を解決する第1の発明は、固有識別子を有する管理対象無線基地局を含む無線通信システムであって、無線フレームに含まれる前記固有識別子に基づいて不正無線局の有無を検出する不正無線局検出手段を含むことを特徴とする。

[0011] 上記課題を解決する第2の発明は、上記第1の発明において、前記不正無線局検出手段は、前記固有識別子と予め登録されている固有識別子とを比較する比較手段と、この比較結果に基づいて前記不正無線局の判定をなす手段とを有することを特徴とする。

[0012] 上記課題を解決する第3の発明は、上記第1又は第2の発明において、前記固有識別子は、互いに通信する無線通信端末、無線基地局のグループを基本サービスセットとしたとき、この基本サービスセット識別のための識別子（BSS識別子）であることを特徴とする。

[0013] 上記課題を解決する第4の発明は、上記第3の発明において、前記不正無線局検出手段は、前記BSS識別子から前記不正無線局の種別を判定する手段を更に有することを特徴とする。

[0014] 上記課題を解決する第5の発明は、上記第3又は第4の発明において、前記不正無線局検出手段は、前記BSS識別子から前記不正無線局の製造元を判定する手段を、更に有することを特徴とする。

[0015] 上記課題を解決する第6の発明は、上記第1から第5のいずれかの発明において、システムによって管理され、無線フレームを取得して前記固有識別子を得る手段を有する管理対象無線基地局を含み、前記不正無線局検出手段は、前記管理対象無線基地局から前記固有識別子を得る手段を更に有することを特徴とする。

[0016] 上記課題を解決する第7の発明は、上記第1から第5のいずれかの発明において、システムによって管理され、無線フレームを取得して前記固有識別子を得る手段を有する管理対象無線通信端末を含み、前記不正無線局検出手段は、前記管理対象無線通信端末から前記固有識別子を得る手段を更に有することを特徴とする。

[0017] 上記課題を解決する第8の発明は、上記第1から第6のいずれかの発明において、前記不正無線局検出手段は、前記不正無線局に接続された管理対象無線通信端

末に対して前記不正無線局の利用を禁止する旨の通知をなす手段を、更に有することを特徴とする。

[0018] 上記課題を解決する第9の発明は、上記第1から第6のいずれかの発明において、スイッチ装置を更に含み、前記不正無線局検出手段は、前記不正無線局に接続された不正無線通信端末のアドレスを検出して、前記スイッチ装置に対して前記アドレスを通知する手段を更に有し、前記スイッチ装置は、前記アドレスを含む無線フレームの廃棄をなす手段を有することを特徴とする。

[0019] 上記課題を解決する第10の発明は、上記第1から第6のいずれかの発明において、前記不正無線局検出手段は、前記管理対象無線基地局に対して前記不正無線通信端末を通知し、また前記管理対象無線基地局に接続された管理対象無線通信端末に対して前記不正無線局を通知する手段を更に有することを特徴とする。

[0020] 上記課題を解決する第11の発明は、上記第1から第6のいずれかの発明において、前記不正無線局検出手段は、前記管理対象無線基地局に接続された不正無線通信端末の通信を不能とするよう制御する手段を更に有することを特徴とする。

[0021] 上記課題を解決する第12の発明は、上記第1から第6のいずれかの発明において、前記不正無線局検出手段は、前記不正無線局の周囲の管理対象無線基地局に対して、前記無線フレームから取得された前記不正無線局のサービスセット識別のための識別子（SS識別子）を通知する手段を更に有し、前記SS識別子の通知を受けた管理対象無線基地局は、前記SS識別子と同一の値を使用して接続した無線通信端末からの無線フレームを受信した場合、この無線フレームを破棄する手段を有することを特徴とする。

[0022] 上記課題を解決する第13の発明は、固有識別子を有する管理対象無線基地局を含む無線通信システムにおける運用管理装置であって、無線フレームに含まれる固有識別子に基づいて不正無線局の有無を検出する不正無線局検出手段を含むことを特徴とする。

[0023] 上記課題を解決する第14の発明は、上記第13の発明において、前記不正無線局検出手段は、前記固有識別子と予め登録されている固有識別子とを比較する比較手段と、この比較結果に基づいて前記不正無線局の判定をなす手段とを有すること

を特徴とする。

[0024] 上記課題を解決する第15の発明は、上記第13又は第14の発明において、前記固有識別子は、互いに通信する無線通信端末、無線基地局のグループを基本サービスセットとしたとき、この基本サービスセット識別のための識別子（BSS識別子）であることを特徴とする。

[0025] 上記課題を解決する第16の発明は、上記第15の発明において、前記BSS識別子から前記不正無線局の種別を判定する手段を更に含むことを特徴とする。

[0026] 上記課題を解決する第17の発明は、上記第15又は第16の発明において、前記BSS識別子から前記不正無線局の製造元を判定する手段を更に含むことを特徴とする。

[0027] 上記課題を解決する第18の発明は、上記第13から第17のいずれかの発明において、システムによって管理され無線フレームを取得して前記固有識別子を得るようにした管理対象無線基地局から前記固有識別子を得る手段を更に含むことを特徴とする。

[0028] 上記課題を解決する第19の発明は、上記第13から第17のいずれかの発明において、システムによって管理され無線フレームを取得して前記固有識別子を得るようにした管理対象無線通信端末から前記固有識別子を得る手段を更に含むことを特徴とする。

[0029] 上記課題を解決する第20の発明は、上記第13から第18のいずれかの発明において、前記不正無線局に接続された管理対象無線通信端末に対して前記不正無線局の利用を禁止する旨の通知をなす手段を更に含むことを特徴とする。

[0030] 上記課題を解決する第21の発明は、上記第13から第18のいずれかの発明において、前記不正無線局に接続された不正無線通信端末のアドレスを検出して、前記スイッチ装置に対して前記アドレスを通知する手段を更に含むことを特徴とする。

[0031] 上記課題を解決する第22の発明は、上記第13から第18のいずれかの発明において、前記管理対象無線基地局に対して前記不正無線通信端末を通知し、また前記管理対象無線基地局に接続された管理対象無線通信端末に対して前記不正無線局を通知する手段を更に含むことを特徴とする。

[0032] 上記課題を解決する第23の発明は、上記第13から第18のいずれかの発明において、前記管理対象無線基地局に接続された不正無線通信端末の通信を不能とするよう制御する手段を更に含むことを特徴とする。

[0033] 上記課題を解決する第24の発明は、上記第13から第18のいずれかの発明において、前記不正無線局の周囲の管理対象無線基地局に対して、前記無線フレームから取得された前記不正無線局のサービスセット識別のための識別子（SS識別子）を通知する手段を、更に含むことを特徴とする。

[0034] 上記課題を解決する第25の発明は、固有識別子を有する管理対象無線基地局と、システムを運用管理する運用管理装置とを含む無線通信システムにおける無線基地局であって、無線フレームから前記固有識別子を取得する手段と、前記固有識別子を、不正無線局の有無検出のために前記運用管理装置へ通知する手段とを含むことを特徴とする。

[0035] 上記課題を解決する第26の発明は、上記第25の発明において、前記運用管理装置から不正無線通信端末の通知を受けて、前記不正無線通信端末の通信を不能とする手段を更に含むことを特徴とする。

[0036] 上記課題を解決する第27の発明は、上記第25又は第26の発明において、前記運用管理装置から前記不正無線局のサービスセット識別のための識別子（SS識別子）の通知を受け、前記SS識別子と同一の値を使用して接続した無線通信端末からの無線フレームを受信した場合、この無線フレームを破棄する手段を更に含むことを特徴とする。

[0037] 上記課題を解決する第28の発明は、固有識別子を有する管理対象無線基地局と、システムを運用管理する運用管理装置とを含む無線通信システムにおける無線通信端末であって、無線フレームから前記固有識別子を取得する手段と、前記固有識別子を、不正無線局の有無検出のために前記運用管理装置へ通知する手段とを含むことを特徴とする。

[0038] 上記課題を解決する第29の発明は、上記第28の発明において、前記運用管理装置から通知された前記不正無線局の利用を禁止する手段を更に含むことを特徴とする。

[0039] 上記課題を解決する第30の発明は、固有識別子を有する管理対象無線基地局を含む無線通信システムにおける不正無線局検出方法であって、無線フレームに含まれる固有識別子に基づいて不正無線局の有無を検出するステップを含むことを特徴とする。

[0040] 上記課題を解決する第31の発明は、固有識別子を有する管理対象無線基地局と、システムを運用管理する運用管理装置とを含む無線通信システムにおける無線基地局の動作制御方法であって、無線フレームから前記固有識別子を取得するステップと、前記固有識別子を、不正無線局の有無検出のために前記運用管理装置へ通知するステップとを含むことを特徴とする。

[0041] 上記課題を解決する第32の発明は、固有識別子を有する管理対象無線基地局と、システムを運用管理する運用管理装置とを含む無線通信システムにおける無線通信端末の動作制御方法であって、無線フレームから前記固有識別子を取得するステップと、前記固有識別子を、不正無線局の有無検出のために前記運用管理装置へ通知するステップとを含むことを特徴とする。

[0042] 上記課題を解決する第33の発明は、固有識別子を有する管理対象無線基地局を含む無線通信システムにおける不正無線局検出方法をコンピュータに実行させるためのプログラムであって、無線フレームに含まれる固有識別子に基づいて不正無線局の有無を検出する処理を含むことを特徴とする。

[0043] 上記課題を解決する第34の発明は、固有識別子を有する管理対象無線基地局と、システムを運用管理する運用管理装置とを含む無線通信システムにおける無線基地局の動作制御方法をコンピュータに実行させるためのプログラムであって、無線フレームから前記固有識別子を取得する処理と、前記固有識別子を、不正無線局の有無検出のために前記運用管理装置へ通知する処理とを含むことを特徴とする。

[0044] 上記課題を解決する第35の発明は、固有識別子を有する管理対象無線基地局と、システムを運用管理する運用管理装置とを含む無線通信システムにおける無線通信端末の動作制御方法をコンピュータに実行させるためのプログラムであって、無線フレームから前記固有識別子を取得する処理と、前記固有識別子を、不正無線局の有無検出のために前記運用管理装置へ通知する処理とを含むことを特徴とする。

[0045] 本発明の作用を述べる。管理対象の無線局が、複数の周波数チャネルにわたり無線空間を検索し、空間を伝搬しているフレームから各基地局に固有のIDであるBSS識別子とフレーム送信元識別子とを取得し、運用管理装置はこれら取得されたBSS識別子と管理対象の基地局として登録された基地局のBSS識別子とを比較することで、不正無線局を検出する。また、取得されたフレーム送信元識別子を用いてその種別や製造元をも判定する。更に、運用管理装置は、この不正無線局の存在を管理対象(正規)無線基地局、管理対象端末、スイッチ装置などへ通知し、不正無線局からのフレーム破棄や通信切断などを指示して、不正無線局との通信不能の対策を可能とする。

発明の効果

[0046] 本発明の監視システムによれば、不正無線局が無線空間に送出するフレームから、各無線局の固有の識別子であるBSS識別子を取得し、このBSS識別子に基づいて不正無線局を特定しているので、不正ユーザ等による詐称等を許さず、不正な基地局を検出することが可能となる。また、BSS識別子の一部から該不正無線局の製造元を示す組織名を判定し、該組織名を判定しているので、不正無線局を絞り込んでから探査することが可能になる。

[0047] また、不正無線局に接続している端末のフレーム送信元識別子を取得し、該フレーム送信元識別子を有線LANスイッチに設定し、該有線LANスイッチを経由するフレームの送信元識別子が一致した場合にはフレームを破棄することにより不正無線局に接続している端末と有線網内のノードとの通信を阻害することが可能になる。

図面の簡単な説明

[0048] [図1]本発明が適用される無線LAN監視システムである。

[図2]実施例1，2の無線LAN監視システムの各構成要素の機能ブロックである。

[図3]実施例1，2の無線LAN監視システムの処理フローである。

[図4]実施例1，2の無線LAN監視システムの処理フローにおける運用管理装置の処理フローである。

[図5]実施例1，2の無線LAN監視システムの処理フローにおける運用管理装置の処理フローである。

[図6]管理対象AP、不正APと端末の接続・設置を示す例である。

[図7]管理対象APとSWの設置位置を示す例である。

[図8]運用管理装置が保持する各種情報リストの例である。

[図9]管理対象APとSWの設置位置と不正APの近傍を示す例である。

[図10]実施例3の無線LAN監視システムの処理フローである。

[図11]実施例3の無線LAN監視システムの各構成要素の機能ブロックである。

[図12]実施例3の無線LAN監視システムの処理フローにおける運用管理装置の処理フローである。

[図13]実施例3の無線LAN監視システムの処理フローにおける運用管理装置の処理フローである。

[図14]実施例3の運用管理装置が保持する各種情報リストの例である。

[図15]実施例4の無線LAN監視システムの各構成要素の機能ブロックである。

[図16]実施例4の運用管理装置に保持されるカンパニーIDリストの例である。

[図17]実施例5の無線LAN監視システムの処理フローである。

[図18]実施例5の無線LAN監視システムの各構成要素の機能ブロックである。

[図19]実施例5の運用管理装置に保持される受信可能BSS識別子リストBの例である。

[図20]実施例5の無線LAN監視システムの処理フローにおける運用管理装置の処理フローである。

[図21]実施例5の無線LAN監視システムの処理フローにおける運用管理装置の処理フローである。

符号の説明

[0049] 100 無線LAN運用管理装置

101 管理対象APリスト(BSS識別子)

102 受信可能BSS識別子リスト

103 不正APリスト

104 不正ad-hocリスト

105 不正AP利用端末リスト

106 管理対象APリスト(AP識別子)

107 管理対象端末リスト(端末識別子)

108 演算処理部

109 AP設置位置リスト

110 SW設置位置リスト

111 送受信部

112 不正AP検出端末リスト

113 監視処理実行部

114 フレーム送信元識別子リスト

115 不正AP検出APリスト

116 カンパニーIDリスト

200 表示装置

201 表示部

202 送受信部

300 管理対象無線LANアクセスポイント

301 有線送受信部

302 BSS識別子格納部

303 不正無線局リスト

304 無線送受信部

305 フレーム送信元識別子リスト

306 受信可能BSS識別子リスト

307 検索処理実行部

308 フィルタリング識別子格納部

309 不正無線局SSID格納部

400 管理対象無線LANクライアント端末

401 無線送受信部

402 検索処理実行部

403 受信可能BSS識別子リスト

404 フレーム送信元識別子リスト

405 メッセージ受信・表示部

406 所属BSS識別子格納部

407 受信可能BSS識別子リスト

500 不正無線局

501 アドホック網を構成する無線LANクライアント端末

502 アドホック網を構成する無線LANクライアント端末

503 不正無線LANアクセスポイント(インフラモード)

504 不正無線LAN端末(アドホックモード)

600 有線LANスイッチ

601 送受信部

602 演算処理部

603 フィルタリング識別子格納部

発明を実施するための最良の形態

[0050] 次に、本発明の実施の形態について図面を参照して詳細に説明する。図1は本発明が適用される無線LAN監視システムの構成を示す図である。無線LANの運用管理を行う運用管理装置100、運用管理情報を表示する表示装置200、管理対象のAP300(アクセスポイントであり、無線基地局)、管理対象の無線通信端末(以下、単に端末と称す)400、APと有線網を接続するスイッチ(SW)600、管理対象外の不正無線局500から構成される。不正無線局500は、管理対象クライアント端末同士501,502が接続されたアドホック網、インフラストラクチャモードで動作する管理対象外のAP503(以降不正APと称す)、アドホックモードで動作する有線網に接続された端末504のいずれか、あるいは組み合わせで存在する。

[0051] 図2は無線LAN監視システムの各構成要素の本発明に関連する機能ブロックを示した図である。運用管理装置100は、管理対象APの個々の無線インタフェースを識別するための情報を格納する管理対象APリスト(BSS識別子)101、管理対象外端末から取得した受信可能BSS識別子を格納する受信可能BSS識別子リストB102、不正APの情報を格納する不正APリスト103、不正ad-hocの情報を格納する不正

ad-hocリスト104、不正APを利用している端末の情報を格納する不正AP利用端末リスト105、不正APを検出した端末の情報を格納する不正AP検出端末リスト112、管理対象APを識別するための情報を格納する管理対象APリスト(AP識別子)106、管理対象端末を識別するための情報を格納する管理対象端末リスト(端末識別子)107、演算処理を行う演算処理部108、APの設置位置情報を格納するAP設置位置リスト109、SWの設置位置情報を格納するSW設置位置リスト110、他の構成要素と通信する送受信部111、監視の制御を行う監視処理実行部113、端末からのフレーム送信元識別子情報を格納するフレーム送信元識別子リストB114から構成される。

[0052] 表示装置200は、運用管理情報を表示する表示部201と他の構成要素と通信する送受信部202から構成される。AP300は有線側の他の構成要素と通信する有線送受信部301、該AP300に割り当てられたBSS識別子を格納するBSS識別子格納部302、不正無線局の情報を格納する不正無線局リスト303、無線側の他の構成要素と通信する無線送受信部304から構成される。

[0053] 管理対象クライアント端末400はAPと通信する無線送受信部401、管理対象クライアント端末の周囲に存在する無線LANを検索する検索処理実行部402、検索結果のBSS識別子情報を格納する受信可能BSS識別子リストA403、検索結果のフレーム送信元識別子を格納するフレーム送信元識別子リスト404、他の構成要素から通知されるメッセージを受信・表示するメッセージ受信・表示部405、該クライアント端末が所属するAPのBSS識別子を格納する所属BSS識別子格納部406、接続先から除外するための識別子リストが格納される不正無線局リスト407から構成される。

[0054] SW600は他の構成要素と通信する送受信部601、演算処理を行う演算処理部602、パケットフィルタリングを行う際にフィルタリング対象を識別するための識別子を格納するフィルタイリング識別子格納部603から構成される。

[0055] 図3は本発明が適用される無線LAN監視システムの処理フローを示した図である。管理対象端末による情報取得処理と運用管理装置による情報に基づく監視・制御処理の2つの独立した処理に分けられる。運用管理装置からの指示で管理対象端末が動作する連携処理も可能であるが、以下では独立した処理として説明する。また、図4、図5は処理フロー中の運用管理装置内の動作を示した図である。図6は管理対象

AP（三角印）と不正AP（星印）と端末（方形印）とが混在する場合の例である。端末と管理対象APあるいは不正APとの間に引かれた線は、端末とAP間の接続関係を表している。図7（a）は、管理対象APとSWの物理的配置を表した図であり、領域を複数のブロック（B4−1ーB4−24）に分けて示している例、（b）、（c）がそれぞれSW、APの設置位置をブロック単位で示した図である。

[0056] 管理対象クライアント端末の検索処理実行部402は、定期的に無線送受信部401を通じて、周囲の無線環境の情報取得を起動する。情報取得はその時点で管理対象クライアント端末が使用している周波数チャネルだけでなく、他のチャネルに対しても行う。管理対象APや不正無線局は管理用やデータのフレームを送信（図3の701）しており、管理対象クライアント端末はこれらフレームを取得し、フレームから取得したBSS識別子は受信可能BSS識別子リストA403に格納する。フレームから取得したBSS識別子とそのフレーム送信元装置の識別子とそのフレームが端末からAPへのフレームか、APから端末へのフレームかを識別する情報をフレーム送信元識別子リスト404に格納する。

[0057] 運用管理装置は、管理対象APのBSS識別子の取得（図3の702、図4の801（この801の詳細説明は実施例の項で後述））を行う。なお、図3では、管理対象APを正規APとして示しており、他の図でも同様とする。監視処理実行部113は、管理対象APリスト（AP識別子）106（図8（a））に記載されたAPに対してBSS識別子を要求する。APはBSS識別子格納部302の情報を運用管理装置に応答し、運用管理装置は取得した情報を管理対象APリスト（BSS識別子）101に格納する。なお、管理対象APリスト（BSS識別子）は予め作成して運用管理装置が保持していても良い。

[0058] 次に受信可能BSS識別子の取得（図3の703、図4の802（この802の詳細説明は実施例の項で後述））を行う。監視処理実行部113は、管理対象端末リスト（端末識別子）107に記載された端末に対して受信可能BSS識別子を要求する。管理対象端末は受信可能BSS識別子リストA403の情報と所属BSS識別子格納部406の情報を運用管理装置に応答し、運用管理装置は取得した情報を受信可能BSS識別子リストB102（図8（b））に格納する。

[0059] 監視処理実行部113は、不正APリスト、不正Ad−hocリスト、不正AP検出端末リスト

を作成する(図4の803(この803の詳細説明は実施例の項で後述))。管理対象APリスト(BSS識別子)101のBSS識別子と受信可能BSS識別子リストB102のBSS識別子を比較し、管理対象APリスト(BSS識別子)101に存在しないBSS識別子を抽出する。BSS識別子に含まれるBSS種別がAPの場合には、不正APリスト103(図8(c))に受信可能BSS識別子および不正APを検出した端末の所属するAPのBSS識別子を、それぞれ不正AP BSS識別子および検出BSS識別子として格納する。また、該不正APを検出した管理対象端末の情報を不正AP検出端末リスト112(図8(d))に格納する。BSS種別がアドホックの場合には、不正Ad-hocリスト104に受信可能BSS識別子および不正Ad-hocを検出した管理対象端末の所属するAPのBSS識別子を格納する。以上の処理により、不正AP、不正Ad-hocが検出できる。

[0060] 次に、以下では、上記手法によって検出された不正AP、不正Ad-hocの情報を利用して、これら不正AP等と接続する端末を検出し、更に検出された端末が管理対象の端末か否かを判定し、不正なものを切り離す処理につき説明する。

[0061] 監視処理実行部113は、不正APを検出した管理対象端末が所属する管理対象APに不正APリスト103に記載された情報を通知する(図3の704、図5の901)。通知を受けた管理対象APは不正無線局リスト303に情報を格納し、定期的あるいは外部からの指示により不正無線局の情報を接続している管理対象クライアント端末に通知する(図3の705)。通知を受けた管理対象端末は、メッセージ受信・表示部405に不正無線局の情報を表示し、ユーザに対して不正無線局が存在することを通知するとともに、不正無線局リスト407に不正無線局の情報を格納する。管理対象端末は以後の接続の際に登録された不正無線局リストの無線局(基地局または端末)には接続しないようにする。

[0062] 次にフレーム送信元識別子の取得(図3の706、図5の902(この902の詳細は実施例の項で後述))を行う。監視処理実行部113は、不正AP検出端末リスト112(図8の(d))に記載された管理対象端末に対して、端末からAPに流れているフレームの送信元識別子(不正APを利用している端末の識別子:以下では不正利用端末識別子)を要求する。管理対象端末はフレーム送信元識別子リスト404から所望の情報を取得して運用管理装置に応答する。運用管理装置は取得した情報をフレーム送信

元識別子リストB114(図8の(e))に格納する。

[0063] フレーム送信元識別子リストB114(図8の(e))の不正AP BSS識別子と不正APリスト(図8の(c))から不正APを検出した管理対象端末の所属するBSS識別子を取得し、AP設置位置リスト109(図7の(c))と管理対象APリスト(BSS識別子)101から不正利用端末識別子と該不正利用端末を検出した管理対象端末が所属する管理対象APの位置の関係を不正AP利用端末リスト105(図8の(f))に格納する。更に、管理対象端末リスト107から不正利用端末識別子が管理対象端末の識別子か否かを特定し、不正AP利用端末リスト105(図8の(f))に格納する。なお、図8の(f)では、R-STA-2 が管理対象の端末であるとしている。

[0064] 監視処理実行部113は、不正AP利用端末に対する対策を行う(図5の903(この903の詳細は実施例の項で後述))。不正AP利用端末が管理対象の場合に、連続検出回数がN回未満(Nは自然数)であれば該不正AP利用端末に対して、不正AP利用禁止のメッセージを通知(図3の707)する。不正AP利用端末が管理対象の場合で、かつ連続検出回数がN回以上の場合、あるいは管理対象外の場合は不正AP利用端末の近傍のSWを検索し、該SWに対して不正AP利用端末の識別子を通知(図3の708)する。

[0065] 近傍のSWの検索は、例えば、不正AP利用端末リスト(図8の(f))の位置情報からB4-2とB4-21 を取得し、図7(a)においてその位置周辺のブロック(B4-1ー3 、B4-7ー9 、B4-14 ー16、B4-20ー22)を近傍とし、その中(図9のハッチ部分)に設置されたSW1, 2, 4, 8, 10, 11が通知の対象とする。

[0066] 不正AP利用禁止のメッセージを受けた管理対象端末のメッセージ受信・表示部405は運用管理装置からのメッセージを表示する。また、不正AP利用端末の識別子を受けたSWは、フィルタリング識別子格納部603にその識別子を格納し、以降、送受信部601を経由するフレームの送信元識別子と比較し、フィルタリング識別子格納部603に格納された値と一致した場合には、そのフレームを破棄する。

[0067] 表示装置200は、周期的に運用管理装置の不正APリスト103、不正ad-hocリスト104、不正AP利用端末リスト105を取得(図3の709)し、表示部201に不正無線局の情報を表示する。不正無線局の表示は、BSS種別毎に分類し、それぞれの種別の

下にBSS識別子を表示する。APの場合には、BSS識別子の下に更に階層化して不正APを利用している端末の識別子を記載する。その際に、該端末が監視対象か否かを識別する記号(○×)を付記する(図2)。

実施例 1

[0068] 次に、前述した最良の実施の形態を、更に具体的に実施例として説明する。この実施例1は、不正無線局の検出を端末が行う例である。無線LAN監視システム及び各構成要素の構成は前述の通りである。図3は本発明が適用される無線LAN監視システムの処理フローを示した図である。管理対象端末による情報取得処理と運用管理装置による情報に基づく監視・制御処理の2つの独立した処理に分けられる。運用管理装置からの指示で管理対象端末が動作する連携処理も可能であるが、以下では独立した処理として説明する。

[0069] また、図4、図5は処理フロー中の運用管理装置内の動作を示した図である。図6は管理対象APと不正APと端末が混在する場合の例である。図7(a)は、管理対象APとSWの物理的配置を表した図であり、領域を複数のブロック(B4-1ーB4-24)に分けて示している例、(b)、(c)がそれぞれSW、APの設置位置をブロック単位で示した図である。

[0070] 管理対象クライアント端末の検索処理実行部402は、定期的に無線送受信部401を通じて、周囲の無線環境の情報取得を起動する。情報取得はその時点で管理対象クライアント端末が使用している周波数チャネルだけでなく、他のチャネルに対しても行う。管理対象APや不正無線局はビーコンフレームやプローブフレーム、データフレームを送信(図3の701)しており、管理対象クライアント端末はこれらフレームを取得し、フレームから取得したBSSIDを受信可能BSS識別子リストA403に格納する。フレームから取得したBSSIDとフレーム送信元装置のMACアドレスとそのフレームが端末からAPへのフレームか、APから端末へのフレームかを識別する"To DS "(DS:Distribution System すなわち網を意味する)領域と"From DS "領域をフレーム送信元識別子リスト404に格納する。

[0071] 運用管理装置は、まず管理対象APのBSSIDの取得(図3の702、図4の801)を行う。監視処理実行部113は、管理対象APリスト(AP識別子)106に記載された管

理対象APのIPアドレスに対してBSSIDを要求する(図4の8011)。管理対象APはBSS識別子格納部302に格納されたBSSIDを運用管理装置に応答し、運用管理装置は取得したBSSIDを管理対象APリスト(BSS識別子)101に格納する(図4の8012)。なお、管理対象APリスト(BSS識別子)は予め作成して運用管理装置が保持していても良い。

[0072] 次に受信可能BSSIDの取得(図3の703、図4の802)を行う。監視処理実行部113は、管理対象端末リスト(端末識別子)107に記載された管理対象端末に対して受信可能なBSSIDを要求する。管理対象端末は受信可能BSS識別子リストA403のBSSIDと所属BSS識別子格納部406のBSSIDを運用管理装置に応答し(図4の8021)、運用管理装置は取得した2つのBSSIDを受信可能BSS識別子リストB102に格納する(図4の8022)。

[0073] 監視処理実行部113は、不正APリスト、不正Ad-hocリスト、不正AP検出端末リストを作成する(図4の803)。管理対象APリスト(BSS識別子)101のBSSIDと受信可能BSS識別子リストB102に記載の受信可能BSSIDを比較し(図4の8031)、管理対象APリスト(BSS識別子)101に存在しないBSSIDを抽出する(図4の8032)。

[0074] このBSSIDに含まれる“universal/local ”ビット(IEEE802規格)が0の場合には(図4の8033の“AP”)、不正APリスト103に不正APのBSSIDと、不正APを検出した管理対象端末の所属するAPのBSSIDを格納する(図4の8034, 8035)。“universal/local”ビットが1の場合には(図4の8033の“adhoc”)、不正Ad-hocリスト104に受信可能BSSIDと不正Ad-hocを検出した管理対象端末の所属するAPのBSSIDを格納する(図4の8036)。

[0075] 以上の処理により、不正APの検出が行われることになる。こうして検出された不正APからの情報漏洩防止の処理が必要になるが、この場合、次の4つのケースが考えられ、これ等各ケース毎に、情報漏洩防止対策が相違してくるので、実施例2として、これ等各ケースについて、以下に説明する。

実施例 2

[0076] 上記の4つのケースとは、(1)管理対象APに管理対象端末が接続されているケース、(2)不正APに管理対象端末が接続されているケース、(3)不正APに不正端末

が接続されているケース、(4)管理対象APに不正端末が接続されているケースである。まず、(1)のケースについての情報漏洩防止処理について述べる。

[0077] 監視処理実行部113は、不正APを検出した管理対象端末が所属するAPに不正APリスト103に記載された不正APのBSSIDを通知する(図3の704、図5の901、9011)。通知を受けた管理対象APは不正無線局リスト303に不正APのBSSIDを格納し、定期的あるいは外部からの指示により、接続している管理対象クライアント端末に不正APのBSSIDを通知する(図3の705)。通知を受けた端末は、メッセージ受信・表示部405に不正APのBSSIDを表示し、ユーザに対して不正APが存在することを通知するとともに、不正無線局リスト407に不正APのBSSIDを格納する。管理対象端末は以後の接続の際に登録された不正無線局リストの無線局には接続しないようにする。

[0078] 次にフレーム送信元識別子の取得(図3の706、図5の902)を行う。監視処理実行部113は、不正AP検出端末リスト112(図8の(d))に記載された管理対象端末に対して、端末からAPに流れているフレームの送信元MACアドレス(不正APを利用している端末のMACアドレス:以下では不正利用端末MACアドレス)を要求する。管理対象端末はフレーム送信元識別子リスト404から"To DS "領域の値が1のフレームの送信元MACアドレスを取得して運用管理装置に応答する。

[0079] 運用管理装置は取得したMACアドレスをフレーム送信元識別子リストB114に格納する(図5の9021)。フレーム送信元識別子リストB114(図8の(e))の不正AP BSSIDと不正APリスト(図8の(c))から不正APを検出した管理対象端末の所属するBSSIDを取得し、AP設置位置リスト109(図7の(c))と管理対象APリスト(BSS識別子)101から不正利用端末MACアドレスと該不正利用端末を検出した管理対象端末が所属するAPの位置の関係を不正AP利用端末リスト105(図8の(f))に格納する(図5の9022)。更に、管理対象端末リスト107から不正利用端末MACアドレスが管理対象端末のMACアドレスか否かを特定し(図5の9023)、不正AP利用端末リスト105(図8の(f))に格納する(図5の9024)。なお、図8の(f)では、R-STA-2 が管理対象の端末であるとしている。

[0080] 次に、(2)のケースである不正APに管理対象端末が接続されている場合、及び(3

)のケースである不正APに不正端末が接続されている場合の情報漏洩防止処理について述べる。監視処理実行部113は、不正AP利用端末に対する対策を行う(図5の903)。不正AP利用端末が管理対象の場合に(図5の9031で"Yes":(2)のケースの場合)、連続検出回数がN回未満であれば該不正AP利用端末に対して、不正AP利用禁止のメッセージを通知する(図3の707、図5の9032, 9033)。不正AP利用端末が管理対象の場合で、連続検出回数がN回以上の場合、あるいは管理対象外の場合は((3)のケースの場合)、不正AP利用端末の近傍のSWを検索し(図5の9034)、該SWに対して不正AP利用端末のMACアドレスを通知(図3の708)する(図5の9035)。

[0081] 近傍のSWの検索は、例えば、不正AP利用端末リスト(図8の(f))の位置情報からB4-2とB4-21 を取得し、図7(a)において、その位置周辺のブロック(B4-1ー3 、B4-7ー9 、B4-14 ー16、B4-20ー22)を近傍とし、その中(図9のメッシュ部分)に設置されたSW1, 2, 4, 8, 10, 11が通知の対象とする。

[0082] 不正AP利用禁止のメッセージを受けた管理対象端末のメッセージ受信・表示部405は運用管理装置からのメッセージを表示する。また、不正AP利用端末のMACアドレスを受けたSWは、フィルタリング識別子格納部603にそのMACアドレスを格納し、以降、送受信部601を経由するフレームの送信元MACアドレスと比較し、フィルタリング識別子格納部603に格納された値と一致した場合にはそのフレームを破棄する。

[0083] 表示装置200は、周期的に運用管理装置の不正APリスト103、不正ad-hocリスト104、不正AP利用端末リスト105を取得(図3の709)し、表示部201に不正無線局のBSSIDを表示する。不正無線局の表示は、BSS種別毎に分類し、それぞれの種別の下にBSSIDを表示する。APの場合には、BSSIDの下に更に階層化して不正APを利用している端末のMACアドレスを記載する。その際に、該端末が監視対象か否かを識別する記号(○×)を付記する(図2)。

[0084] (4)のケースである管理対象APに不正端末が接続されている場合について述べる。データパケットヘッダには、送信元アドレスが挿入されており、管理対象APのBSSIDはわかっているので、管理対象APに接続されている端末のMACアドレスが分か

る。よって、このMACアドレスを、運用管理装置に登録されている端末のアドレスと比較することにより、不正端末か否かが特定可能である。そこで、管理対象APに接続されている不正端末に対しては、通信を不可能とする処置をとることで、情報漏洩が可能となる。そのための例として、先述した様に、SWにおいてフィルタリングをかけてフレーム破棄を行う方法や、管理対象APに対して回線の切断指示をなす方法や、このAP自身でフィルタリングを行ってフレーム破棄をなす方法などがある。

[0085] なお、上記の管理対象APの判定は、固有識別子であるBSSIDを利用することにより判定ができるものであり、詐称が容易なSSIDでは、不正APや端末の特定ができず、よって、上記の各(1)ー(4)にそれぞれ対応する情報漏洩防止対策は困難となり、上記の特許文献1におけるSSIDを用いる方式は、実用的ではない。

[0086] 先の実施例1では、不正無線局の情報としてBSSIDのみを取得して、表示装置に表示、管理対象APへ通知したが、BSSIDにあわせてSSIDも取得し、表示、通知しても良い。また、管理対象端末への不正無線局のBSSIDの通知は、管理対象APを経由して行われるとして説明したが、運用管理装置から管理対象端末に直接通知しても良い。

[0087] 更に、実施例1では検出結果を表示装置に表示したが、検出結果を表示装置に表示するのではなく、予め定められた通信手段を利用して、管理者に通知してもよい。通信手段には、例えば、電話や電子メールなどが考えられる。また、実施例1では、不正無線局の検出、検出した結果の通知、検出した結果に基づく制御の全てを行うように記載したが、例えば、不正無線局の検出のみ、というように一部の処理のみを実行するシステムでもよい。更に利用者の設定により、一部または全部の処理を選択的に実行できる機能を備えても良い。

実施例 3

[0088] 実施例1では、不正無線局の検出を管理対象端末が行っていたが、不正無線局の検出を管理対象APが行うことも考えられる。図10は本実施例の処理フローを示す図である。実施例1の処理フローとの違いは、受信可能BSS識別子の取得(図10の710)とフレーム送信元識別子の取得(図10の711)が運用管理装置と管理対象APの間で行われている点である。

[0089] 図11は無線LAN監視システムの各構成要素の実施例3に関連する機能ブロックを示す図である。実施例1の機能ブロックとの違いは、実施例1では管理対象端末に存在した検索処理実行部402、受信可能BSS識別子リストAとフレーム送信元識別子リスト404が不要になり、管理対象APに検索処理実行部307、受信可能BSS識別子リストA306とフレーム送信元識別子リスト305が存在する点、及び運用管理装置に不正AP検出端末リスト112が不要になり、不正AP検出APリスト115が存在する点である。

[0090] 図12、図13は処理フロー中の運用管理装置の動作を示す図でり、図4、図5と同等部分は同一符号にて示している。実施例1との違いは、図12の804、803と、図13の905である。図12の804は、管理対象APリストに記載の管理対象APの全IPアドレスに対して、受信可能BSSIDと該APのBSSIDを要求し(図12の8041)、取得したBSSIDを受信可能BSS識別子リストB102に出力する(図12の8042)。

[0091] 図12の803は、受信可能BSS識別子リストBのBSSIDと管理対象APリスト(BSS識別子)と比較を行い(図12の8032)、管理対象に含まれていないBSSIDでかつ、BSS種別がAPと判定された場合には(図12の8033)、不正APに該BSSIDを書き出し(図12の8034)、更に不正AP検出APリストに不正APを検出した管理対象APのBSSIDを書き出す(図12の8037)。図14は受信可能BSS識別子リストB及び不正AP検出APリストの例である。

[0092] 図13は本実施例における情報漏洩防止処理の動作を示すものであり、図5と同等であるが、相違部分を説明する。運用管理装置は管理対象APに不正APのBSSIDを通知する(図13の904)。そして、このAPからフレーム送信元識別子を取得し(図13の9051)、当該APのBSSIDとAP設置位置リストから、APの位置を取得する(図13の9052)。次に、フレーム送信元識別子と管理対象端末リストのエントリを比較して、不正APを利用している端末が登録済みかどうかを判定し(図13の9053)、不正AP利用端末リストにフレーム送信元識別子と検出したAPの位置と登録済みか否かを書き出す(図13の9054)。処理903は図5のそれと同一である。

実施例 4

[0093] 次に、不正APの表示にBSSIDだけでなく、カンパニー名を付記する実施例につ

いて説明する。先の実施例1では、不正APの表示にBSSIDを使用していたが、一般に人が識別し辛いBSSIDに加えて、識別しやすい該不正APの製造元の組織名を付記することも考えられる。図15は無線LAN監視システムの各構成要素の実施例4に関連する機能ブロックを示す図である。実施例1との機能ブロックの違いは、運用管理装置にカンパニーIDリスト116が追加されている点である。カンパニーIDリストの例を図16に示す。カンパニーIDは3バイトの16進で表現される値であり、組織名は製造元を表す文字列である。

[0094] 表示装置200は、運用管理装置から不正APリスト、不正ad-hocリストに加えて、カンパニーIDリストを取得する。BSSIDの先頭から3バイトはカンパニーIDであるため、取得した不正APリストのBSSIDの先頭3バイトに一致するエントリをカンパニーIDリストから検索する。不正APを表示する際に検索して得たベンダー名をBSSIDの後に付記する。

[0095] 具体的には、図15で表示されている不正APのBSSIDは、01:23:45:67:89:ab、00:11:22:33:44:55 、00:66:77:88:99:aa であり、各先頭の3バイトのカンパニーIDは01:23:45、00:11:22、00:66:77である。各カンパニーIDをキーにして図16から各不正APの製造元はそれぞれcompnay1、company2、company3であることを判定し、表示部に組織名を表示する。なお、BSSIDと組織名との対応は表示装置内で行うように説明したが、運用管理装置側で行っても良い。

実施例 5

[0096] 次に、不正APが出現した場合、不正APを検出した周囲の管理対象APに不正APと同じSSIDを設定する実施例について述べる。すなわち、先の実施例1では、不正APに接続する端末のMACアドレスを検出して、そのMACアドレスをSWに設定することにより、SWで不正APに接続した端末からのフレームを破棄するようにしていたが、不正APに接続しようとする管理対象外端末を管理対象APに接続させて、その管理対象外端末からのフレームを管理対象APで破棄することも考えられる。

[0097] 図17は実施例5の処理フローを示す図である。実施例1の処理フローとの違いは、運用管理装置と管理対象端末の間で行われるフレーム送信元識別子の取得706、運用管理装置と不正APに接続した管理対象端末との間で行われる不正無線局利

用禁止のメッセージ通知707、運用管理装置とSWの間で行われる不正利用端末識別子の通知708が削除され、運用管理装置と管理対象APの間で行われる不正無線局SSID713通知が追加されたことである。

[0098] 図18は無線LAN監視システムの各構成要素の実施例4に関連する機能ブロックを示す図である。実施例1との機能ブロックの違いは、管理対象端末のフレーム送信元識別子リストが不要な点、管理対象端末の受信可能BSS識別子リストA403には、受信可能BSSIDに加えて、該BSSIDを持つ不正無線局のSSIDも格納される点、同様に運用管理装置の受信可能BSS識別子リストBに不正無線局のSSIDが格納(図19)される点、管理対象APに不正無線局のSSIDを格納する不正無線局SSID格納部309、不正無線局SSID格納部に格納されたSSIDを使用して接続している管理対象外端末のMACアドレスを格納するフィルタリング識別子格納部308が追加された点である。

[0099] 図20、図21は処理フロー中の運用管理装置の動作を示す図であり、図20において、図4と同等部分は同一符号にて示している。実施例1との違いは、図20の805と、図21の906の処理が追加・変更されている点、図5の902、903が削除されている点である。図20の805では、運用管理装置は管理対象端末から受信可能BSSIDに加えてSSIDを取得し(図20の8051)、受信可能BSS識別子リストBに格納している(図20の8052)。図21の906では、運用管理装置は、不正APを検出した管理対象端末が所属する管理対象APに対して、その管理対象APに接続する端末が検出した不正APのSSIDを通知する(図20の9061, 9062)。

[0100] 無線LANを利用しようとする端末は、一般に周囲を検索して受信可能なSSIDを取得し、その中で所望のSSIDの無線LANに接続を試みる。そのため、不正APを使用した有線網への不正侵入は、不正APを設置し、その不正APに接続して有線網に侵入するという手順になる。

[0101] 本実施例では、運用管理装置が管理対象端末から不正APのSSIDを取得(図17の712)し、取得した不正APのSSIDを管理対象APに設定(図17の713、図21の9062)する。管理対象APは該SSIDをビーコンに載せて送信するため、BSSIDは異なるが同一のSSIDを持ったAPが複数存在する環境が構築され、不正APに接続し

ようとする端末が不正APに接続できる頻度は低くなる。管理対象APに接続される場合もあり、その場合には該端末と有線網との通信は遮断されることになる。

[0102] 以上述べたように、本発明によれば、固有のBSS識別子を不正無線局の判定に使用することにより、SS識別子を詐称したアクセスポイントやSS識別子を隠蔽するアクセスポイントも不正無線局として検出・表示することが可能となる。また、不正無線局の表示を種別毎に行うことによって、探査する対象の絞込みが行え、不正無線局の探査・撤去作業が改善される。更に、不正APに接続した端末の識別子を取得し、該識別子をキーにしてアクセスポイントあるいは有線LANスイッチによりフレームを破棄することにより、不正APを経由して有線網にアクセスされ情報が漏洩されることを防止できセキュリティが向上する。

[0103] 上述した各動作フローは、予め記録媒体にプログラムとして動作手順を格納しておき、これをコンピュータにより読み取って実行させるようにすることができるものである。

請求の範囲

[1] 固有識別子を有する管理対象無線基地局を含む無線通信システムであって、無線フレームに含まれる前記固有識別子に基づいて不正無線局の有無を検出する不正無線局検出手段を含むことを特徴とする無線通信システム。

[2] 前記不正無線局検出手段は、前記固有識別子と予め登録されている固有識別子とを比較する比較手段と、この比較結果に基づいて前記不正無線局の判定をなす手段とを有することを特徴とする請求項1に記載の無線通信システム。

[3] 前記固有識別子は、互いに通信する無線通信端末、無線基地局のグループを基本サービスセットとしたとき、この基本サービスセット識別のための識別子（BSS識別子）であることを特徴とする請求項1に記載の無線通信システム。

[4] 前記不正無線局検出手段は、前記BSS識別子から前記不正無線局の種別を判定する手段を更に有することを特徴とする請求項3に記載の無線通信システム。

[5] 前記不正無線局検出手段は、前記BSS識別子から前記不正無線局の製造元を判定する手段を、更に有することを特徴とする請求項3に記載の無線通信システム。

[6] システムによって管理され、無線フレームを取得して前記固有識別子を得る手段を有する管理対象無線基地局を含み、

前記不正無線局検出手段は、前記管理対象無線基地局から前記固有識別子を得る手段を、更に有することを特徴とする請求項1に記載の無線通信システム。

[7] システムによって管理され、無線フレームを取得して前記固有識別子を得る手段を有する管理対象無線通信端末を含み、

前記不正無線局検出手段は、前記管理対象無線通信端末から前記固有識別子を得る手段を、更に有することを特徴とする請求項1に記載の無線通信システム。

[8] 前記不正無線局検出手段は、前記不正無線局に接続された管理対象無線通信端末に対して前記不正無線局の利用を禁止する旨の通知をなす手段を更に有することを特徴とする請求項1に記載の無線通信システム。

[9] スイッチ装置を更に含み、

前記不正無線局検出手段は、前記不正無線局に接続された不正無線通信端末のアドレスを検出して、前記スイッチ装置に対して前記アドレスを通知する手段を、更に

有し、

前記スイッチ装置は、前記アドレスを含む無線フレームの廃棄をなす手段を有することを特徴とする請求項1に記載の無線通信システム。

[10] 前記不正無線局検出手段は、前記管理対象無線基地局に対して前記不正無線通信端末を通知し、また前記管理対象無線基地局に接続された管理対象無線通信端末に対して前記不正無線局を通知する手段を更に有することを特徴とする請求項1に記載の無線通信システム。

[11] 前記不正無線局検出手段は、前記管理対象無線基地局に接続された不正無線通信端末の通信を不能とするよう制御する手段を更に有することを特徴とする請求項1に記載の無線通信システム。

[12] 前記不正無線局検出手段は、前記不正無線局の周囲の管理対象無線基地局に対して、前記無線フレームから取得された前記不正無線局のサービスセット識別のための識別子（SS識別子）を通知する手段を、更に有し、

前記SS識別子の通知を受けた管理対象無線基地局は、前記SS識別子と同一の値を使用して接続した無線通信端末からの無線フレームを受信した場合、この無線フレームを破棄する手段を有することを特徴とする請求項1に記載の無線通信システム。

[13] 固有識別子を有する管理対象無線基地局を含む無線通信システムにおける運用管理装置であって、

無線フレームに含まれる固有識別子に基づいて不正無線局の有無を検出する不正無線局検出手段を含むことを特徴とする運用管理装置。

[14] 前記不正無線局検出手段は、前記固有識別子と予め登録されている固有識別子とを比較する比較手段と、この比較結果に基づいて前記不正無線局の判定をなす手段とを有することを特徴とする請求項13に記載の運用管理装置。

[15] 前記固有識別子は、互いに通信する無線通信端末、無線基地局のグループを基本サービスセットとしたとき、この基本サービスセット識別のための識別子（BSS識別子）であることを特徴とする請求項13に記載の運用管理装置。

[16] 前記BSS識別子から前記不正無線局の種別を判定する手段を更に含むことを特

徴とする請求項15に記載の運用管理装置。

[17] 前記BSS識別子から前記不正無線局の製造元を判定する手段を更に含むことを特徴とする請求項15に記載の運用管理装置。

[18] システムによって管理され無線フレームを取得して前記固有識別子を得るようにした管理対象無線基地局から前記固有識別子を得る手段を更に含むことを特徴とする請求項13に記載の運用管理装置。

[19] システムによって管理され無線フレームを取得して前記固有識別子を得るようにした管理対象無線通信端末から前記固有識別子を得る手段を更に含むことを特徴とする請求項13に記載の運用管理装置。

[20] 前記不正無線局に接続された管理対象無線通信端末に対して前記不正無線局の利用を禁止する旨の通知をなす手段を更に含むことを特徴とする請求項13に記載の運用管理装置。

[21] 前記不正無線局に接続された不正無線通信端末のアドレスを検出して、前記スイッチ装置に対して前記アドレスを通知する手段を更に含むことを特徴とする請求項13に記載の運用管理装置。

[22] 前記管理対象無線基地局に対して前記不正無線通信端末を通知し、また前記管理対象無線基地局に接続された管理対象無線通信端末に対して前記不正無線局を通知する手段を更に含むことを特徴とする請求項13に記載の運用管理装置。

[23] 前記管理対象無線基地局に接続された不正無線通信端末の通信を不能とするよう制御する手段を更に含むことを特徴とする請求項13に記載の運用管理装置。

[24] 前記不正無線局の周囲の管理対象無線基地局に対して、前記無線フレームから取得された前記不正無線局のサービスセット識別のための識別子（SS識別子）を通知する手段を、更に含むことを特徴とする請求項13に記載の運用管理装置。

[25] 固有識別子を有する管理対象無線基地局と、システムを運用管理する運用管理装置とを含む無線通信システムにおける無線基地局であって、

無線フレームから前記固有識別子を取得する手段と、

前記固有識別子を、不正無線局の有無検出のために前記運用管理装置へ通知する手段と

を含むことを特徴とする無線基地局。

[26] 前記運用管理装置から不正無線通信端末の通知を受けて、前記不正無線通信端末の通信を不能とする手段を更に含むことを特徴とする請求項25に記載の無線基地局。

[27] 前記運用管理装置から前記不正無線局のサービスセット識別のための識別子(SS識別子)の通知を受け、前記SS識別子と同一の値を使用して接続した無線通信端末からの無線フレームを受信した場合、この無線フレームを破棄する手段を更に含むことを特徴とする請求項25に記載の無線基地局。

[28] 固有識別子を有する管理対象無線基地局と、システムを運用管理する運用管理装置とを含む無線通信システムにおける無線通信端末であって、

無線フレームから前記固有識別子を取得する手段と、

前記固有識別子を、不正無線局の有無検出のために前記運用管理装置へ通知する手段と

を含むことを特徴とする無線通信端末。

[29] 前記運用管理装置から通知された前記不正無線局の利用を禁止する手段を更に含むことを特徴とする請求項28に記載の無線通信端末。

[30] 固有識別子を有する管理対象無線基地局を含む無線通信システムにおける不正無線局検出方法であって、

無線フレームに含まれる固有識別子に基づいて不正無線局の有無を検出するステップを含むことを特徴とする不正無線局検出方法。

[31] 固有識別子を有する管理対象無線基地局と、システムを運用管理する運用管理装置とを含む無線通信システムにおける無線基地局の動作制御方法であって、

無線フレームから前記固有識別子を取得するステップと、

前記固有識別子を、不正無線局の有無検出のために前記運用管理装置へ通知するステップと

を含むことを特徴とする動作制御方法。

[32] 固有識別子を有する管理対象無線基地局と、システムを運用管理する運用管理装置とを含む無線通信システムにおける無線通信端末の動作制御方法であって、

無線フレームから前記固有識別子を取得するステップと、

前記固有識別子を、不正無線局の有無検出のために前記運用管理装置へ通知するステップと

を含むことを特徴とする動作制御方法。

[33] 固有識別子を有する管理対象無線基地局を含む無線通信システムにおける不正無線局検出方法をコンピュータに実行させるためのプログラムであって、

無線フレームに含まれる固有識別子に基づいて不正無線局の有無を検出する処理を含むことを特徴とするプログラム。

[34] 固有識別子を有する管理対象無線基地局と、システムを運用管理する運用管理装置とを含む無線通信システムにおける無線基地局の動作制御方法をコンピュータに実行させるためのプログラムであって、

無線フレームから前記固有識別子を取得する処理と、

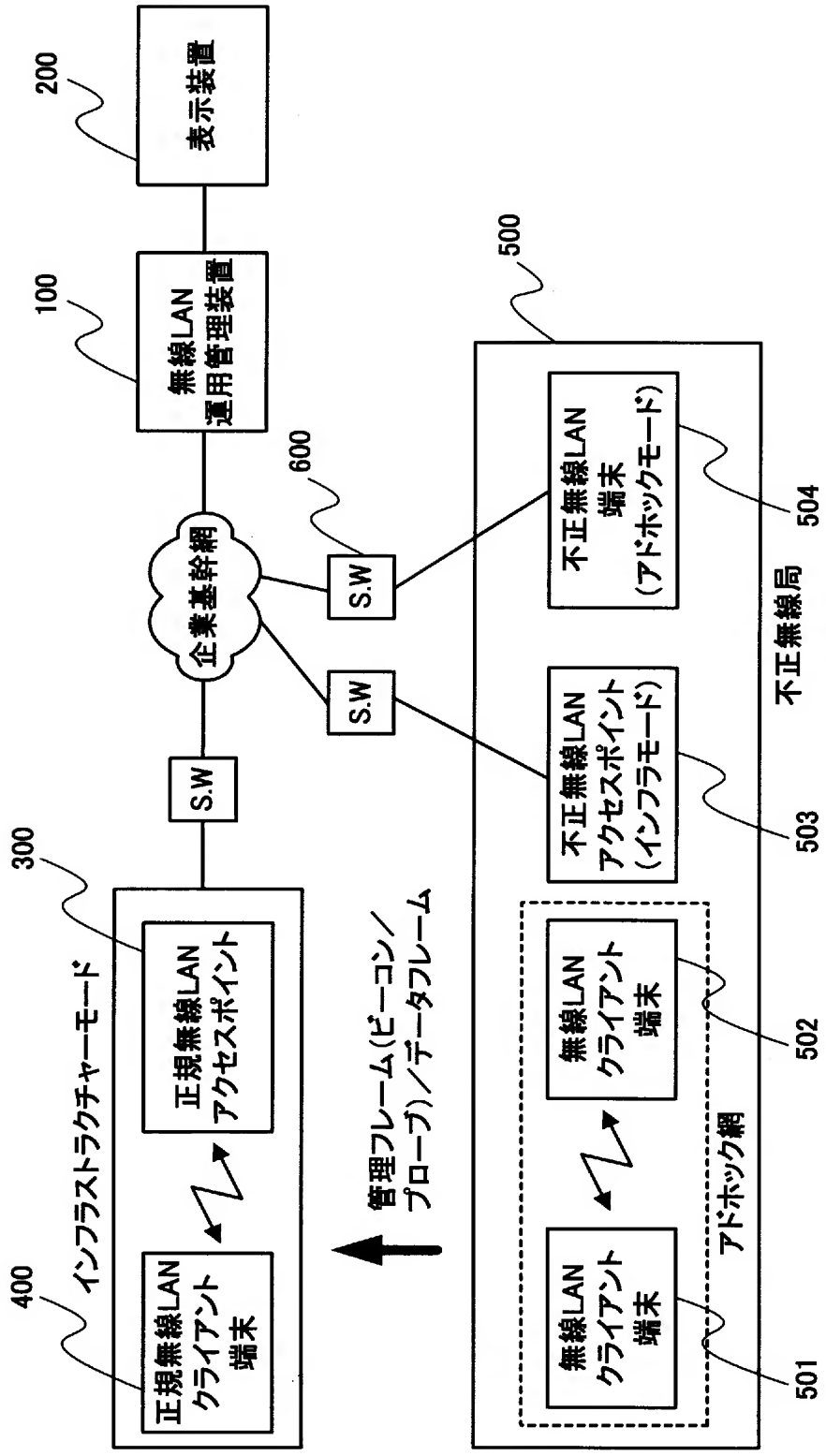
前記固有識別子を、不正無線局の有無検出のために前記運用管理装置へ通知する処理と

を含むことを特徴とするプログラム。

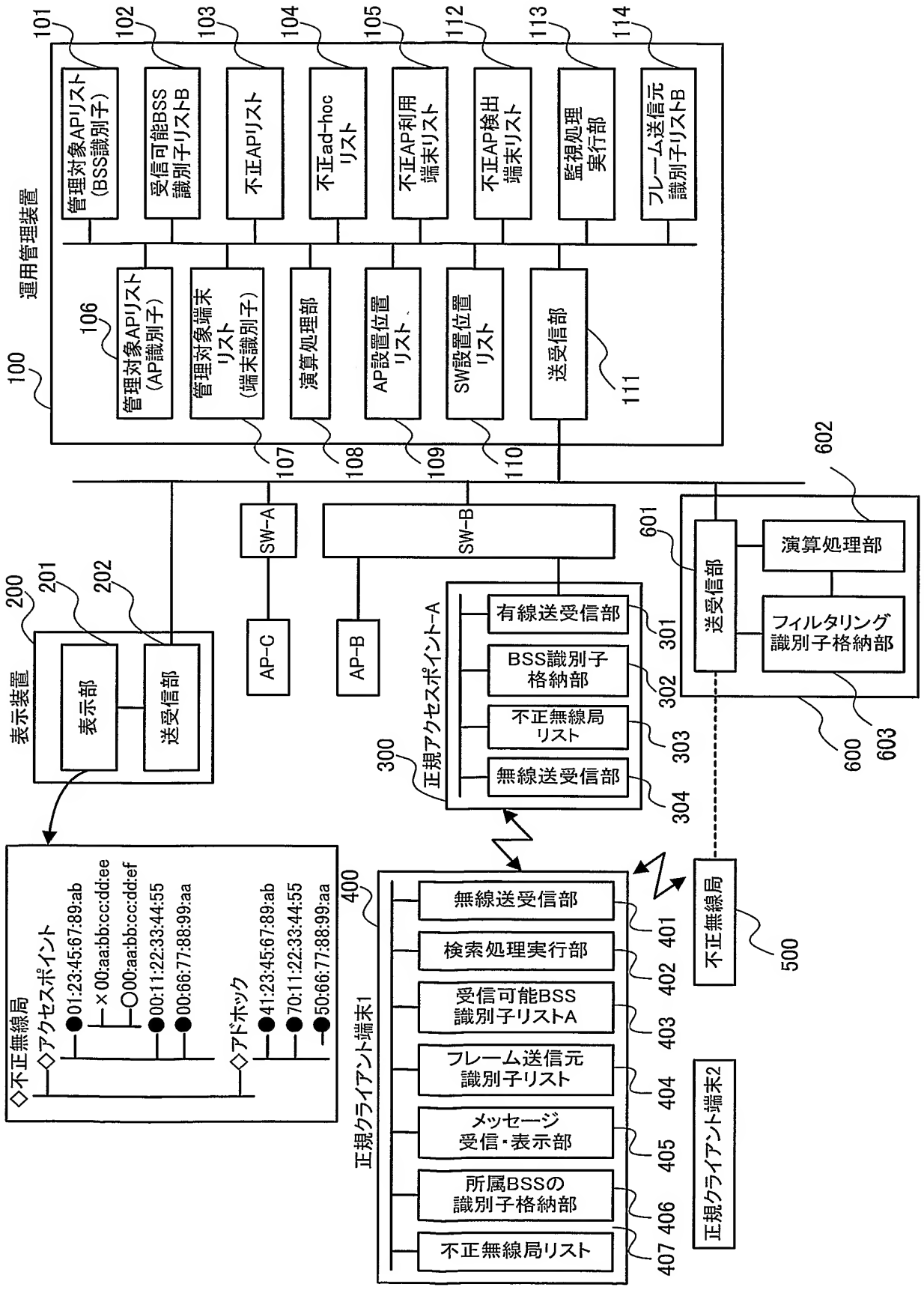
[35] 固有識別子を有する管理対象無線基地局と、システムを運用管理する運用管理装置とを含む無線通信システムにおける無線通信端末の動作制御方法をコンピュータに実行させるためのプログラムであって、

無線フレームから前記固有識別子を取得する処理と、前記固有識別子を、不正無線局の有無検出のために前記運用管理装置へ通知する処理とを含むことを特徴とするプログラム。

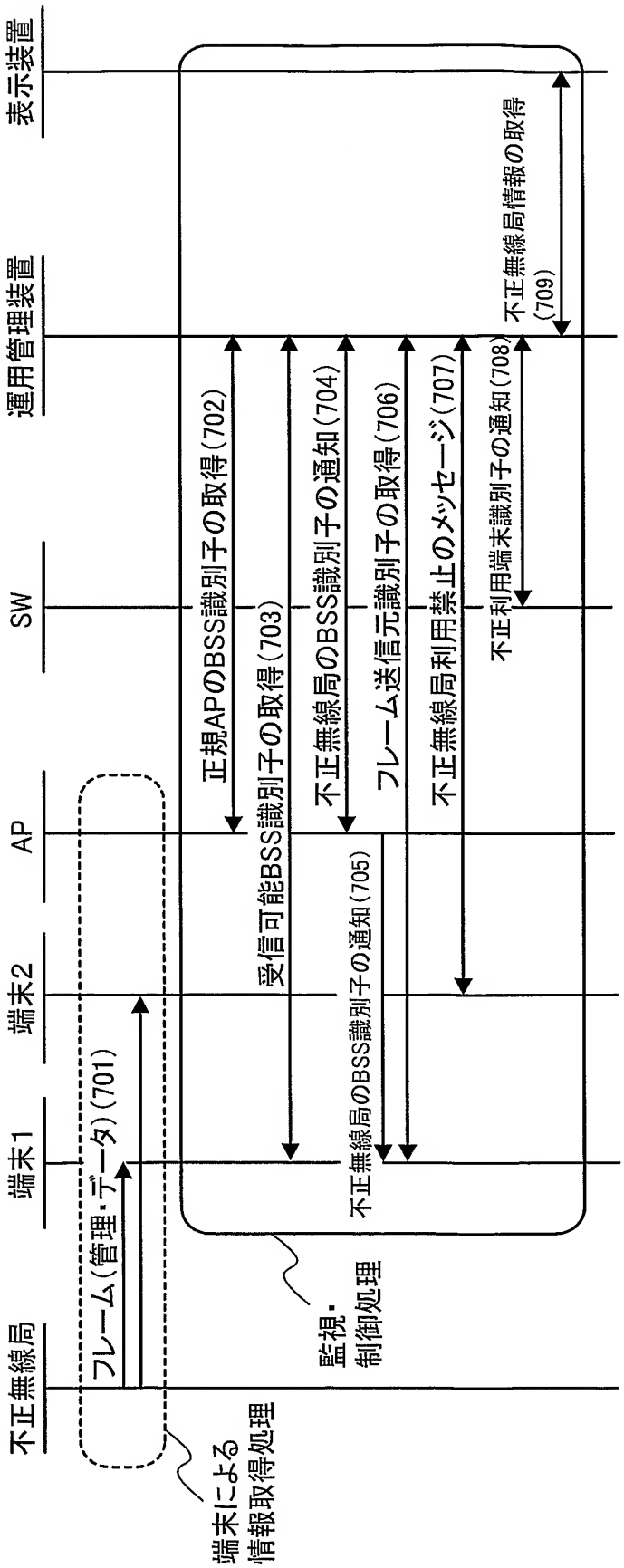
[図1]


200
表示装置
100
無線LAN
運用管理装置
600
企業基幹網
S.W
S.W
S.W
500
不正無線LAN
端末
(アドホックモード)
504
不正無線局
不正無線LAN
アクセスポイント
(インフラモード)
503
300
インフラストラクチャーモード
正規無線LAN
アクセスポイント
管理フレーム(ビーコン/
プローブ)/データフレーム
無線LAN
クライアント
端末
502
アドホック網
400
正規無線LAN
クライアント
端末
無線LAN
クライアント
端末
501

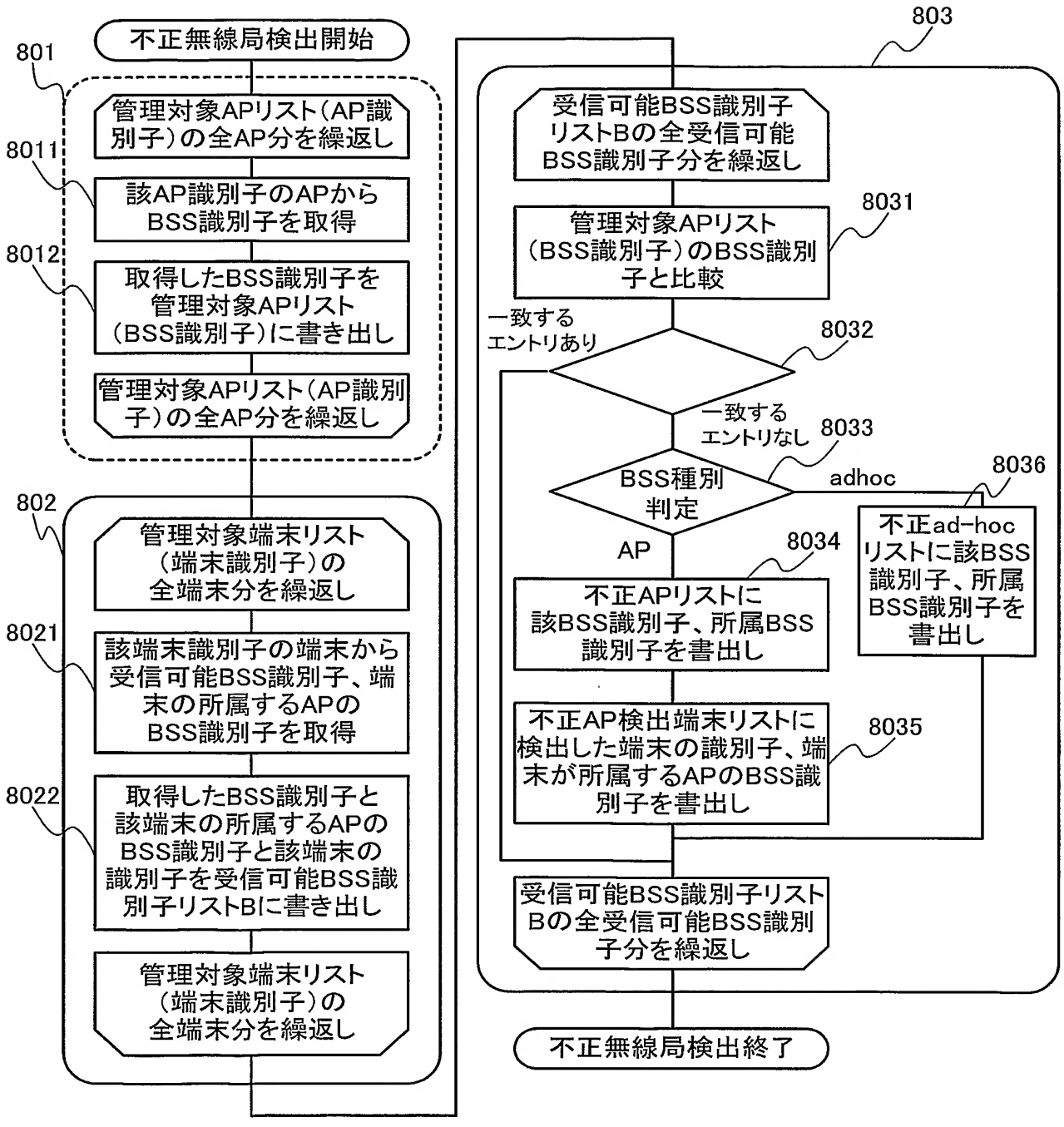
[図2]


運用管理装置
100
101 管理対象APリスト (BSS識別子)
102 受信可能BSS 識別子リストB
103 不正APリスト
104 不正ad-hoc リスト
105 不正AP利用 端末リスト
112 不正AP検出 端末リスト
113 監視処理 実行部
114 フレーム送信元 識別子リストB
106 管理対象APリスト (AP識別子)
管理対象端末 リスト (端末識別子)
演算処理部
AP設置位置 リスト
SW設置位置 リスト
送受信部
111
107
108
109
110
SW-A
SW-B
AP-C
AP-B
200 表示装置
201 表示部
202 送受信部
◇不正無線局
◇アクセスポイント
●01:23:45:67:89:ab
×00:aa:bb:cc:dd:ee
○00:aa:bb:cc:dd:ef
●00:11:22:33:44:55
●00:66:77:88:99:aa
◇アドホック
●41:23:45:67:89:ab
●70:11:22:33:44:55
●50:66:77:88:99:aa
300 正規アクセスポイントA
有線送受信部 301
BSS識別子 格納部 302
不正無線局 リスト 303
無線送受信部 304
400 正規クライアント端末1
無線送受信部 401
検索処理実行部 402
受信可能BSS 識別子リストA 403
フレーム送信元 識別子リスト 404
メッセージ 受信・表示部 405
所属BSSの 識別子格納部 406
不正無線局リスト 407
不正無線局 500
正規クライアント端末2
600
601 送受信部
602 演算処理部
フィルタリング 識別子格納部 603
SW-C

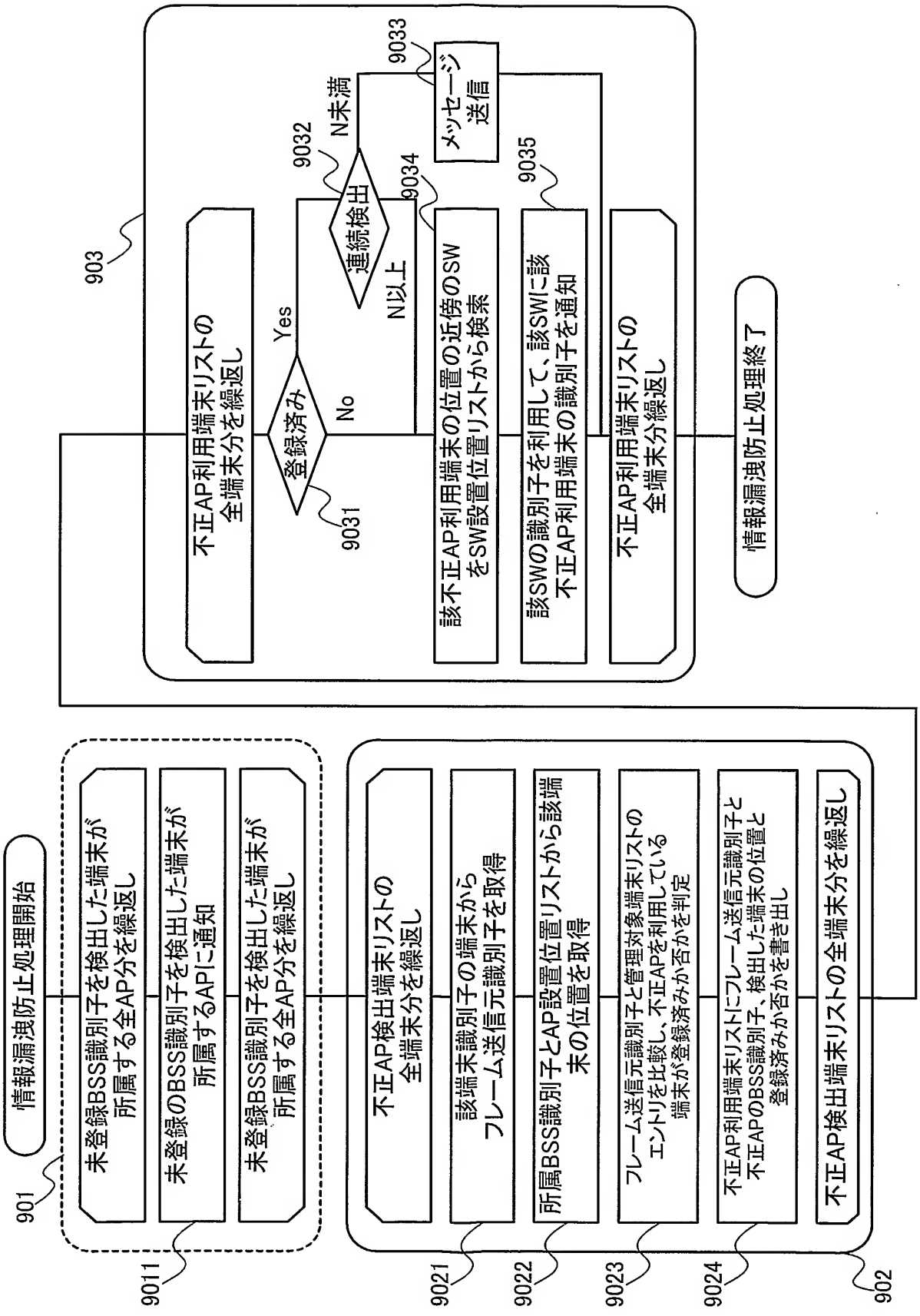
[図3]


不正無線局
端末1
端末2
AP
SW
運用管理装置
表示装置
フレーム(管理・データ)(701)
端末による
情報取得処理
正規APのBSS識別子の取得(702)
受信可能BSS識別子の取得(703)
不正無線局のBSS識別子の通知(704)
不正無線局のBSS識別子の通知(705)
フレーム送信元識別子の取得(706)
不正無線局利用禁止のメッセージ(707)
不正利用端末識別子の通知(708)
不正無線局情報の取得
(709)
監視・
制御処理

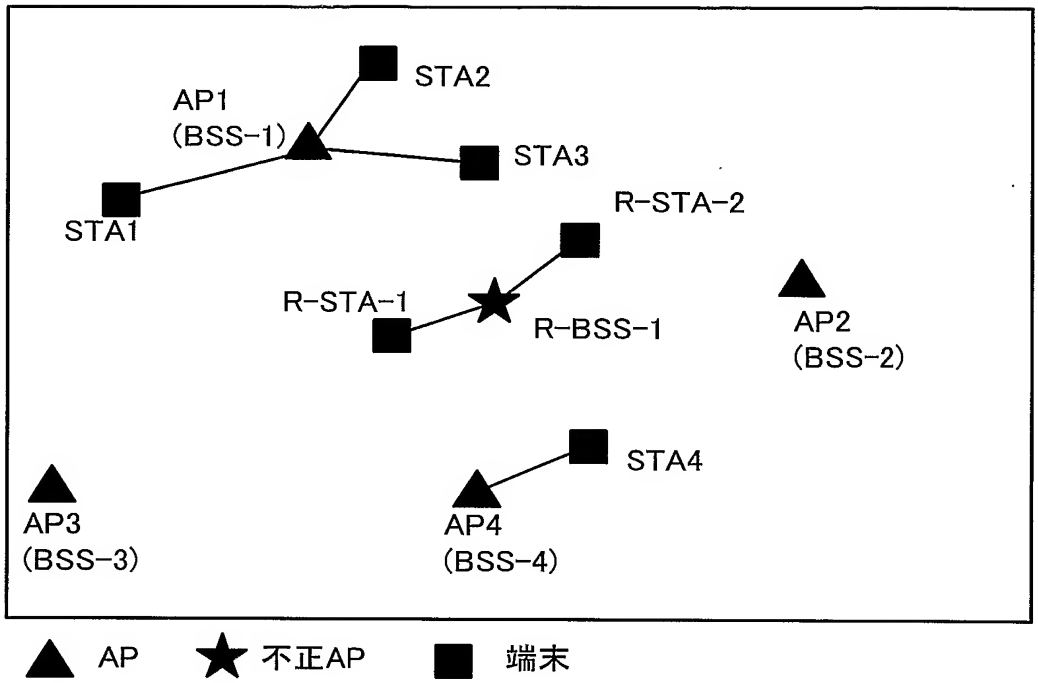
[図4]


不正無線局検出開始
801
管理対象APリスト(AP識別子)の全AP分を繰返し
8011
該AP識別子のAPからBSS識別子を取得
8012
取得したBSS識別子を管理対象APリスト(BSS識別子)に書き出し
管理対象APリスト(AP識別子)の全AP分を繰返し
802
管理対象端末リスト(端末識別子)の全端末分を繰返し
8021
該端末識別子の端末から受信可能BSS識別子、端末の所属するAPのBSS識別子を取得
8022
取得したBSS識別子と該端末の所属するAPのBSS識別子と該端末の識別子を受信可能BSS識別子リストBに書き出し
管理対象端末リスト(端末識別子)の全端末分を繰返し
803
受信可能BSS識別子リストBの全受信可能BSS識別子分を繰返し
8031
管理対象APリスト(BSS識別子)のBSS識別子と比較
一致するエントリあり
8032
一致するエントリなし
8033
BSS種別判定
adhoc
8036
不正ad-hocリストに該BSS識別子、所属BSS識別子を書出し
AP
8034
不正APリストに該BSS識別子、所属BSS識別子を書出し
不正AP検出端末リストに検出した端末の識別子、端末が所属するAPのBSS識別子を書出し
8035
受信可能BSS識別子リストBの全受信可能BSS識別子分を繰返し
不正無線局検出終了

[図5]


901
情報漏洩防止処理開始
9011
未登録BSS識別子を検出した端末が所属する全AP分を繰返し
未登録のBSS識別子を検出した端末が所属するAPIに通知
未登録BSS識別子を検出した端末が所属する全AP分を繰返し
902
9021
不正AP検出端末リストの全端末分を繰返し
9022
該端末識別子の端末からフレーム送信元識別子を取得
9023
所属BSS識別子とAP設置位置リストから該端末の位置を取得
9024
フレーム送信元識別子と管理対象端末リストのエントリを比較し、不正APを利用している端末が登録済みか否かを判定
不正AP利用端末リストにフレーム送信元識別子と不正APのBSS識別子、検出した端末の位置と登録済みか否かを書き出し
不正AP検出端末リストの全端末分を繰返し
903
不正AP利用端末リストの全端末分を繰返し
9031
登録済み
Yes
No
9032
連続検出
N未満
N以上
9033
メッセージ送信
9034
該不正AP利用端末の位置の近傍のSWをSW設置位置リストから検索
9035
該SWの識別子を利用して、該SWに該不正AP利用端末の識別子を通知
不正AP利用端末リストの全端末分繰返し
情報漏洩防止処理終了

[図6]



[図7]

B4-1 SW1	B4-2 AP1	B4-3 SW2	B4-4	B4-5 SW3	B4-6
B4-7	B4-8 SW4	B4-9	B4-10 SW5	B4-11 AP2	B4-12 SW6
B4-13 SW7	B4-14	B4-15 SW8	B4-16	B4-17 SW9	B4-18
AP3 B4-19	B4-20 SW10	AP4 B4-21	B4-22 SW11	B4-23	B4-24 SW12

(a)

AP識別子	位置
SW1	B4-1
SW2	B4-2
SW3	B4-3
SW4	B4-4
SW5	B4-5
SW6	B4-6
SW7	B4-7
SW8	B4-8
SW9	B4-9
SW10	B4-10
SW11	B4-11
SW12	B4-12

(b)

AP識別子	位置
AP1	B4-2
AP2	B4-11
AP3	B4-19
AP4	B4-21

(c)

[図8]

AP識別子	BSS識別子
AP1	BSS-1
AP2	BSS-2
AP3	BSS-3
AP4	BSS-4

(a) 管理対象APリスト(BSS識別子)

端末識別子	所属BSS識別子	受信可能BSS識別子
STA1	BSS-1	
STA2	BSS-1	
STA3	BSS-1	R-BSS-1
STA4	BSS-4	R-BSS-1
		BSS-2

(b) 受信可能BSS識別子リストB

不正AP BSS識別子	検出BSS識別子
R-BSS-1	BSS-1、BSS-4

(c) 不正APリスト

端末識別子	所属BSS識別子
STA3	BSS-1
STA4	BSS-4

(d) 不正AP検出端末リスト

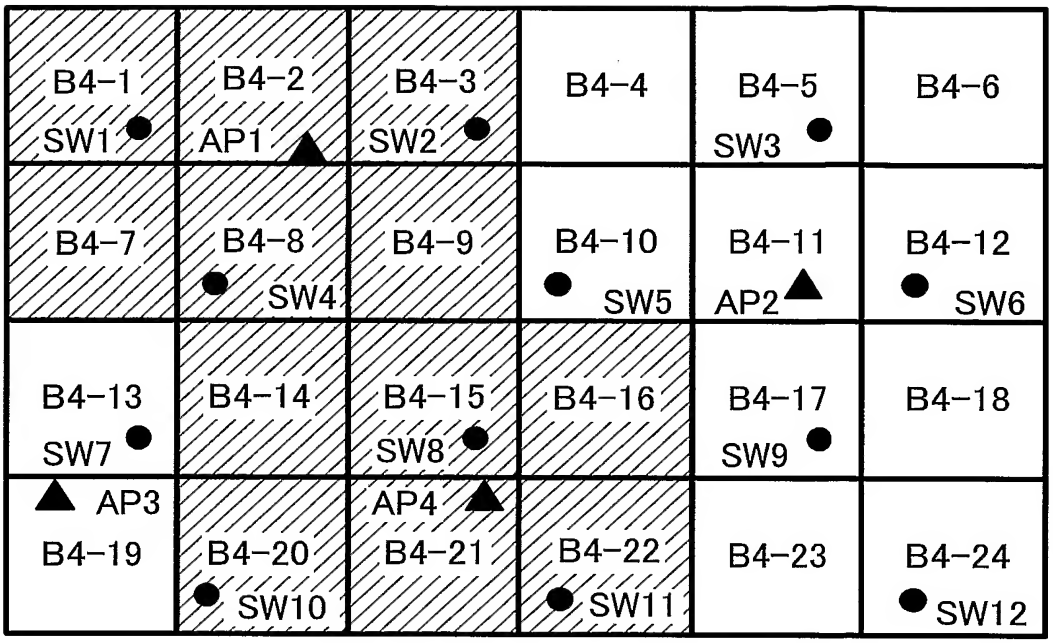
不正AP BSS識別子	不正AP利用端末識別子
R-BSS-1	R-STA-1、R-STA-2、R-STA-3

(e) フレーム送信元識別子リストB

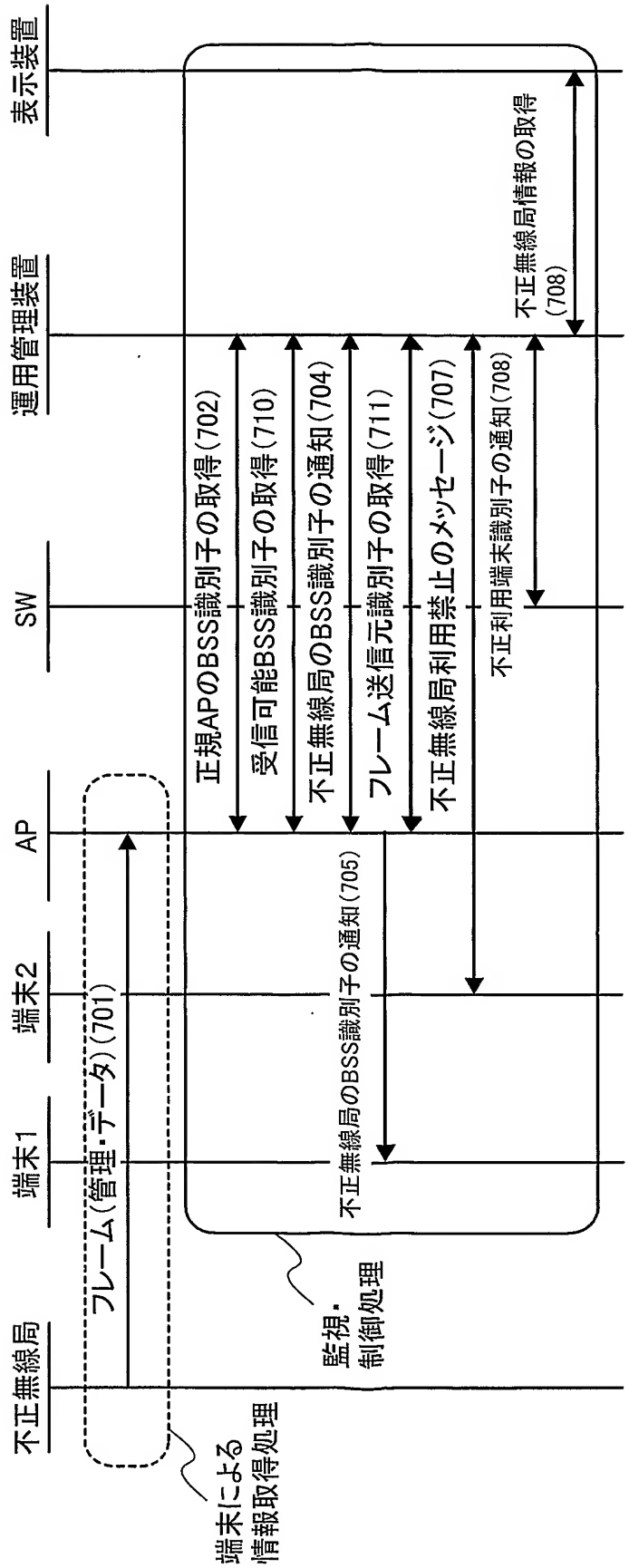
不正AP利用端末識別子	不正AP BSS識別子	位置	登録
R-STA-1	R-BSS-1	B4-2orB4-21	×
R-STA-2	R-BSS-1	B4-2orB4-21	○
R-STA-3	R-BSS-1	B4-2orB4-21	×

(f) 不正AP利用者端末リスト

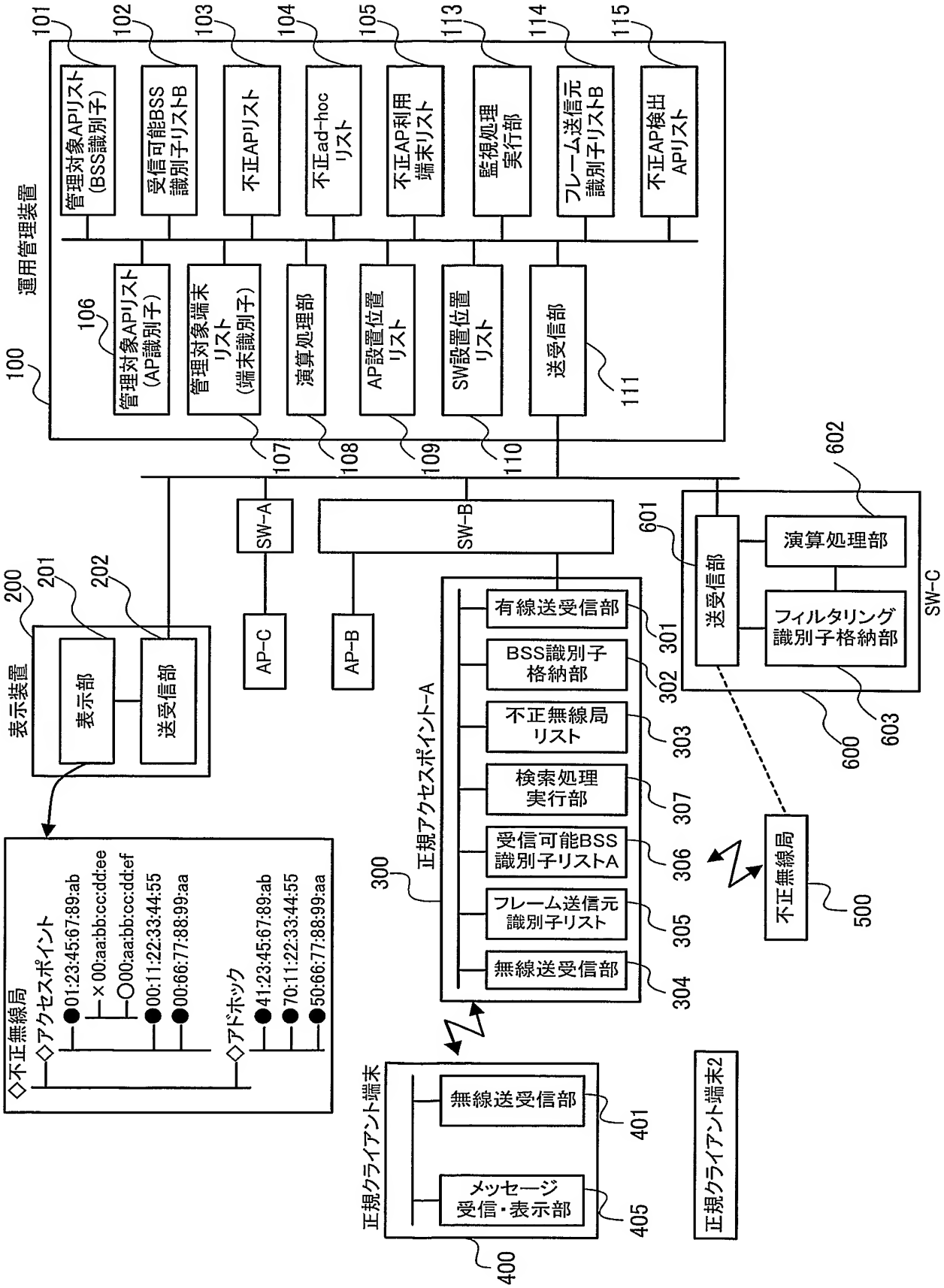
[図9]


B4-1
SW1
B4-2
AP1
B4-3
SW2
B4-4
B4-5
SW3
B4-6
B4-7
B4-8
SW4
B4-9
B4-10
SW5
B4-11
AP2
B4-12
SW6
B4-13
SW7
B4-14
B4-15
SW8
B4-16
B4-17
SW9
B4-18
AP3
B4-19
B4-20
SW10
AP4
B4-21
B4-22
SW11
B4-23
B4-24
SW12

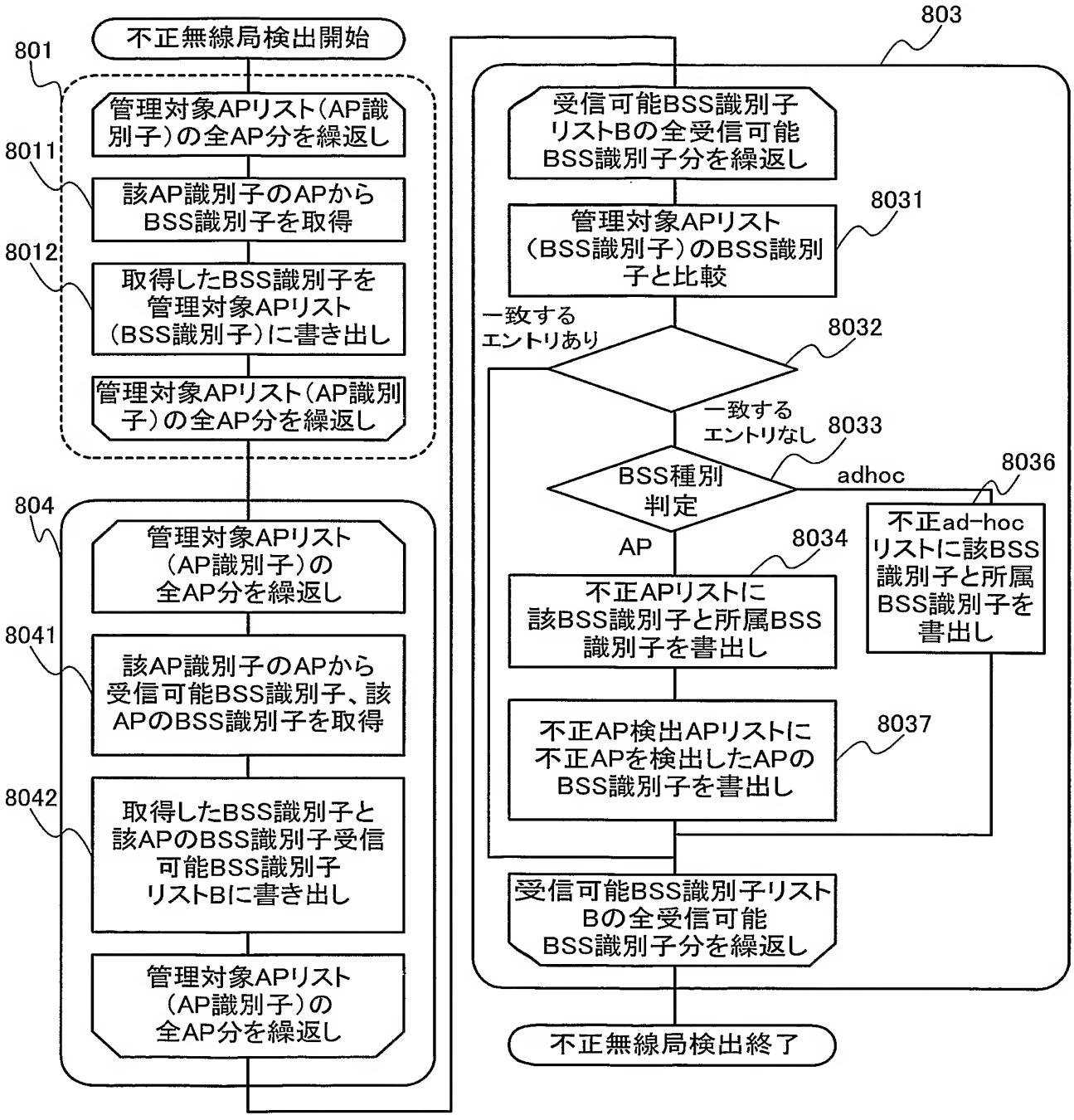
[図10]


不正無線局
端末1
端末2
AP
SW
運用管理装置
表示装置
フレーム(管理・データ)(701)
端末による
情報取得処理
正規APのBSS識別子の取得(702)
受信可能BSS識別子の取得(710)
不正無線局のBSS識別子の通知(704)
フレーム送信元識別子の取得(711)
不正無線局利用禁止のメッセージ(707)
不正利用端末識別子の通知(708)
不正無線局情報の取得
(708)
不正無線局のBSS識別子の通知(705)
監視・
制御処理

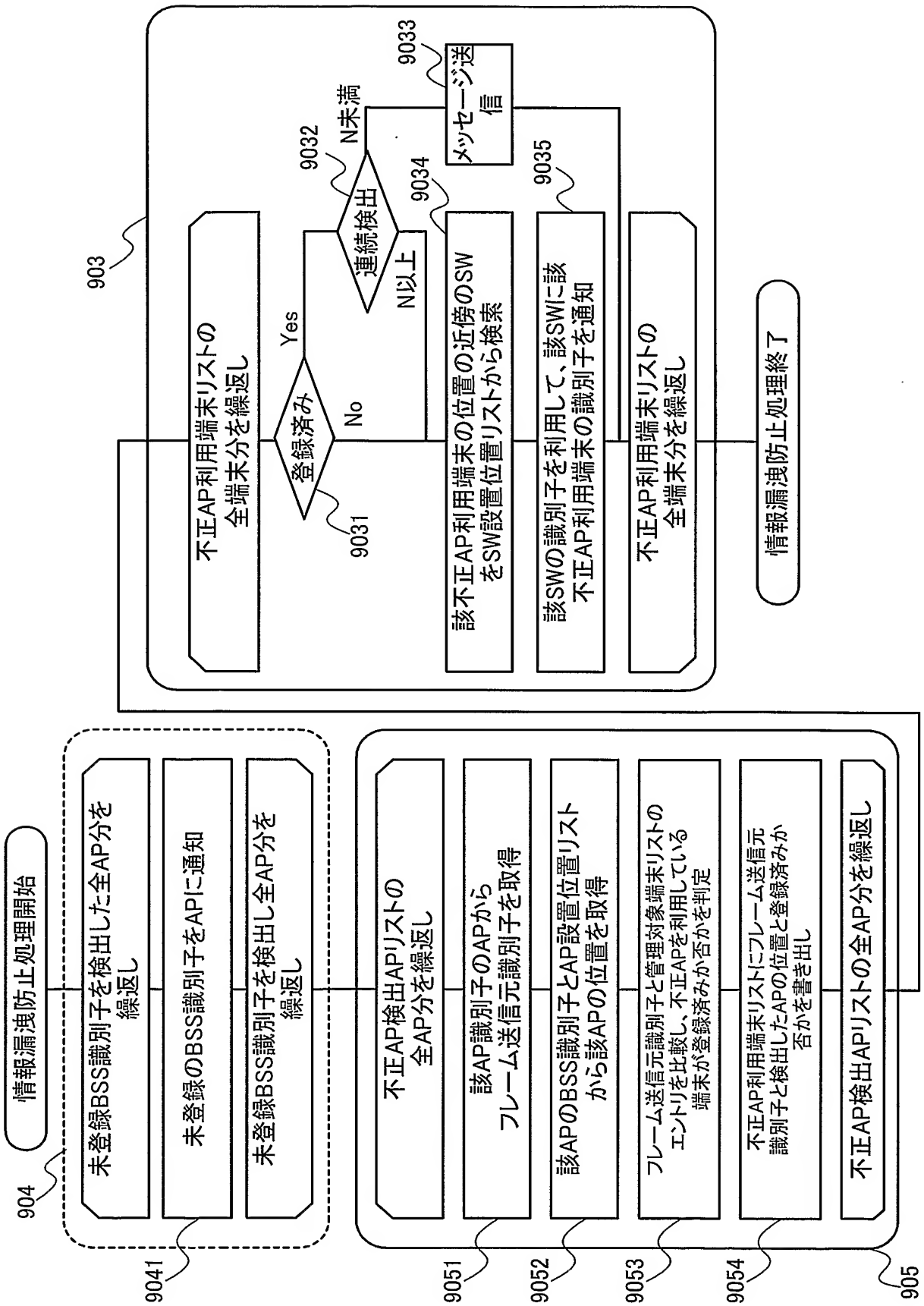
[図11]


運用管理装置
100
管理対象APリスト (BSS識別子)
101
受信可能BSS識別子リストB
102
不正APリスト
103
不正ad-hocリスト
104
不正AP利用端末リスト
105
監視処理実行部
113
フレーム送信元識別子リストB
114
不正AP検出APリスト
115
管理対象APリスト (AP識別子)
106
管理対象端末リスト (端末識別子)
107
演算処理部
108
AP設置位置リスト
109
SW設置位置リスト
110
送受信部
111
SW-A
SW-B
AP-C
AP-B
表示装置
200
表示部
201
送受信部
202
◇不正無線局
◇アクセスポイント
●01:23:45:67:89:ab
×00:aa:bb:cc:dd:ee
○00:aa:bb:cc:dd:ef
●00:11:22:33:44:55
●00:66:77:88:99:aa
◇アドホック
●41:23:45:67:89:ab
●70:11:22:33:44:55
●50:66:77:88:99:aa
正規アクセスポイント-A
300
有線送受信部
301
BSS識別子格納部
302
不正無線局リスト
303
検索処理実行部
307
受信可能BSS識別子リストA
306
フレーム送信元識別子リスト
305
無線送受信部
304
SW-C
602
601
送受信部
演算処理部
フィルタリング識別子格納部
600
603
不正無線局
500
正規クライアント端末
無線送受信部
401
メッセージ受信・表示部
405
400
正規クライアント端末2

[図12]


不正無線局検出開始
801
管理対象APリスト(AP識別子)の全AP分を繰返し
8011
該AP識別子のAPからBSS識別子を取得
8012
取得したBSS識別子を管理対象APリスト(BSS識別子)に書き出し
管理対象APリスト(AP識別子)の全AP分を繰返し
804
管理対象APリスト(AP識別子)の全AP分を繰返し
8041
該AP識別子のAPから受信可能BSS識別子、該APのBSS識別子を取得
8042
取得したBSS識別子と該APのBSS識別子受信可能BSS識別子リストBに書き出し
管理対象APリスト(AP識別子)の全AP分を繰返し
803
受信可能BSS識別子リストBの全受信可能BSS識別子分を繰返し
8031
管理対象APリスト(BSS識別子)のBSS識別子と比較
一致するエントリあり
8032
一致するエントリなし
8033
BSS種別判定
adhoc
8036
不正ad-hocリストに該BSS識別子と所属BSS識別子を書出し
AP
8034
不正APリストに該BSS識別子と所属BSS識別子を書出し
不正AP検出APリストに不正APを検出したAPのBSS識別子を書出し
8037
受信可能BSS識別子リストBの全受信可能BSS識別子分を繰返し
不正無線局検出終了

[図13]


情報漏洩防止処理開始
904
未登録BSS識別子を検出した全AP分を繰返し
未登録のBSS識別子をAPに通知
未登録BSS識別子を検出し全AP分を繰返し
9041
903
不正AP利用端末リストの全端末分を繰返し
登録済み
Yes
No
9031
連続検出
9032
N未満
N以上
9033
メッセージ送信
9034
該不正AP利用端末の位置の近傍のSWをSW設置位置リストから検索
9035
該SWの識別子を利用して、該SWに該不正AP利用端末の識別子を通知
不正AP利用端末リストの全端末分を繰返し
情報漏洩防止処理終了
不正AP検出APリストの全AP分を繰返し
9051
該AP識別子のAPからフレーム送信元識別子を取得
9052
該APのBSS識別子とAP設置位置リストから該APの位置を取得
9053
フレーム送信元識別子と管理対象端末リストのエントリを比較し、不正APを利用している端末が登録済みか否かを判定
9054
不正AP利用端末リストにフレーム送信元識別子と検出したAPの位置と登録済みか否かを書き出し
不正AP検出APリストの全AP分を繰返し
905

[図14]

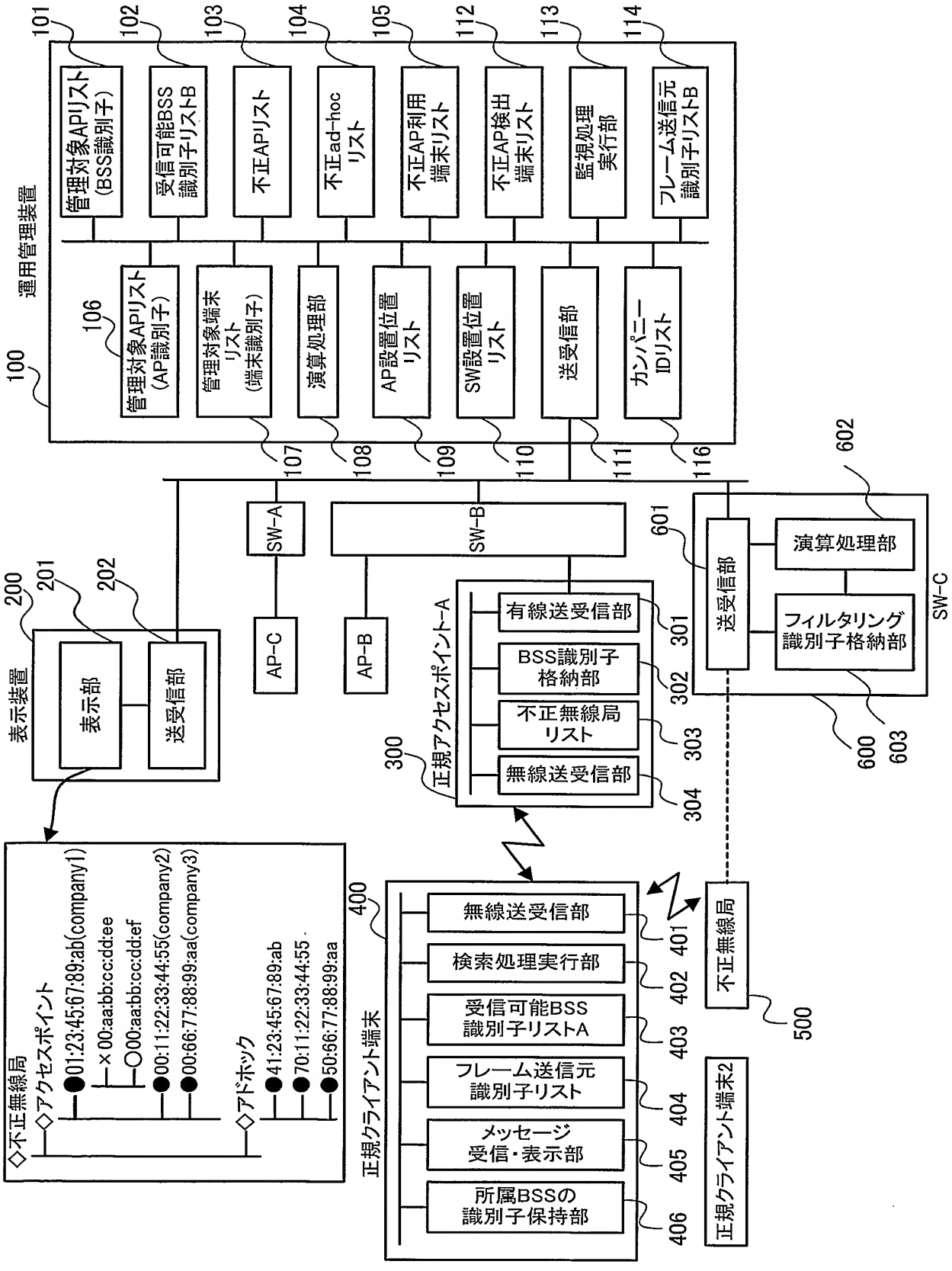
APのBSS識別子	受信可能BSS識別子
BSS−1	R−BSS−1
BSS−4	R−BSS−1

(a) 受信可能BSS識別子リストB

所属BSS識別子
BSS−1
BSS−4

(b) 不正AP検出APリスト

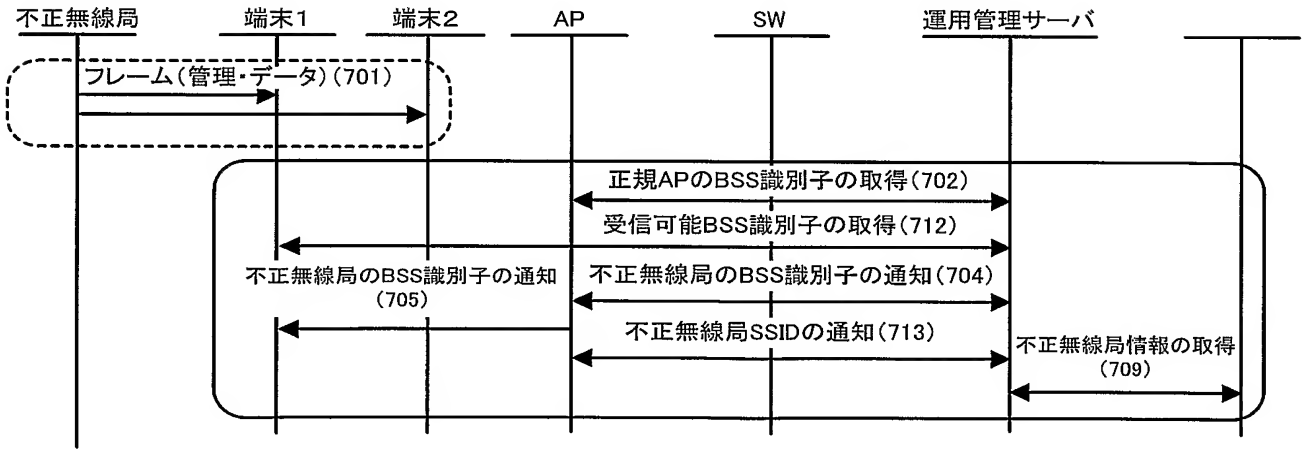
[図15]


運用管理装置
100
101
管理対象APリスト (BSS識別子)
102
受信可能BSS 識別子リストB
103
不正APリスト
104
不正ad-hoc リスト
105
不正AP利用 端末リスト
112
不正AP検出 端末リスト
113
監視処理 実行部
114
フレーム送信元 識別子リストB
106
管理対象APリスト (AP識別子)
管理対象端末 リスト (端末識別子)
演算処理部
AP設置位置 リスト
SW設置位置 リスト
送受信部
カンパニー IDリスト
107
108
109
110
111
116
SW-A
SW-B
AP-C
AP-B
602
601
送受信部
演算処理部
フィルタリング 識別子格納部
SW-C
600
603
200
201
202
表示装置
表示部
送受信部
300
正規アクセスポイント-A
有線送受信部
301
BSS識別子 格納部
302
不正無線局 リスト
303
無線送受信部
304
◇不正無線局
◇アクセスポイント
●01:23:45:67:89:ab(company1)
×00:aa:bb:cc:dd:ee
○00:aa:bb:cc:dd:ef
●00:11:22:33:44:55(company2)
●00:66:77:88:99:aa(company3)
◇アドホック
●41:23:45:67:89:ab
●70:11:22:33:44:55
●50:66:77:88:99:aa
400
正規クライアント端末
無線送受信部
401
検索処理実行部
402
受信可能BSS 識別子リストA
403
フレーム送信元 識別子リスト
404
メッセージ 受信・表示部
405
所属BSSの 識別子保持部
406
不正無線局
500
正規クライアント端末2

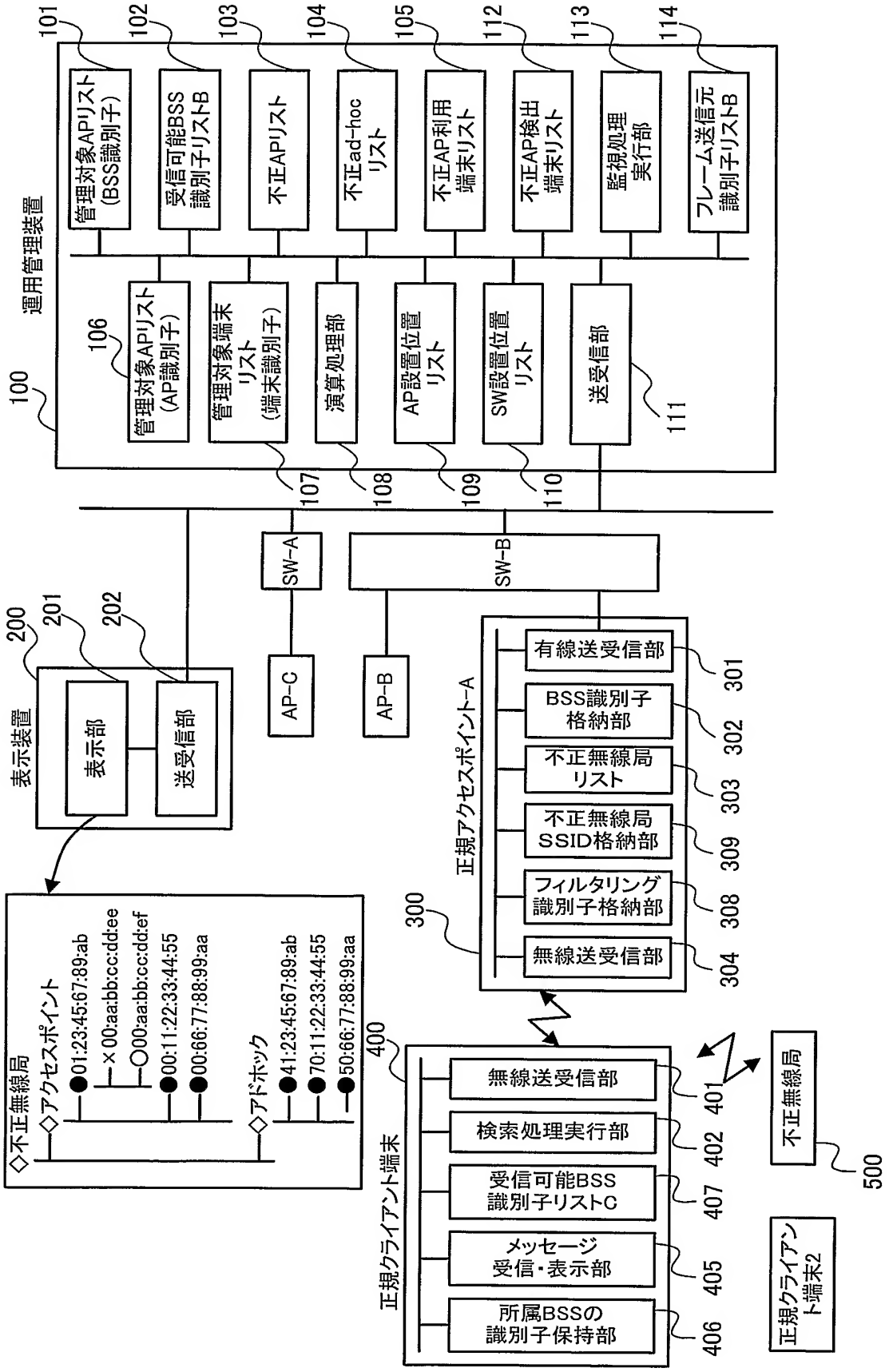
[図16]

カンパニーID	組織名
01:23:45	company1
00:11:22	company2
00:66:77	company3
02:46:8a	company4

[図17]



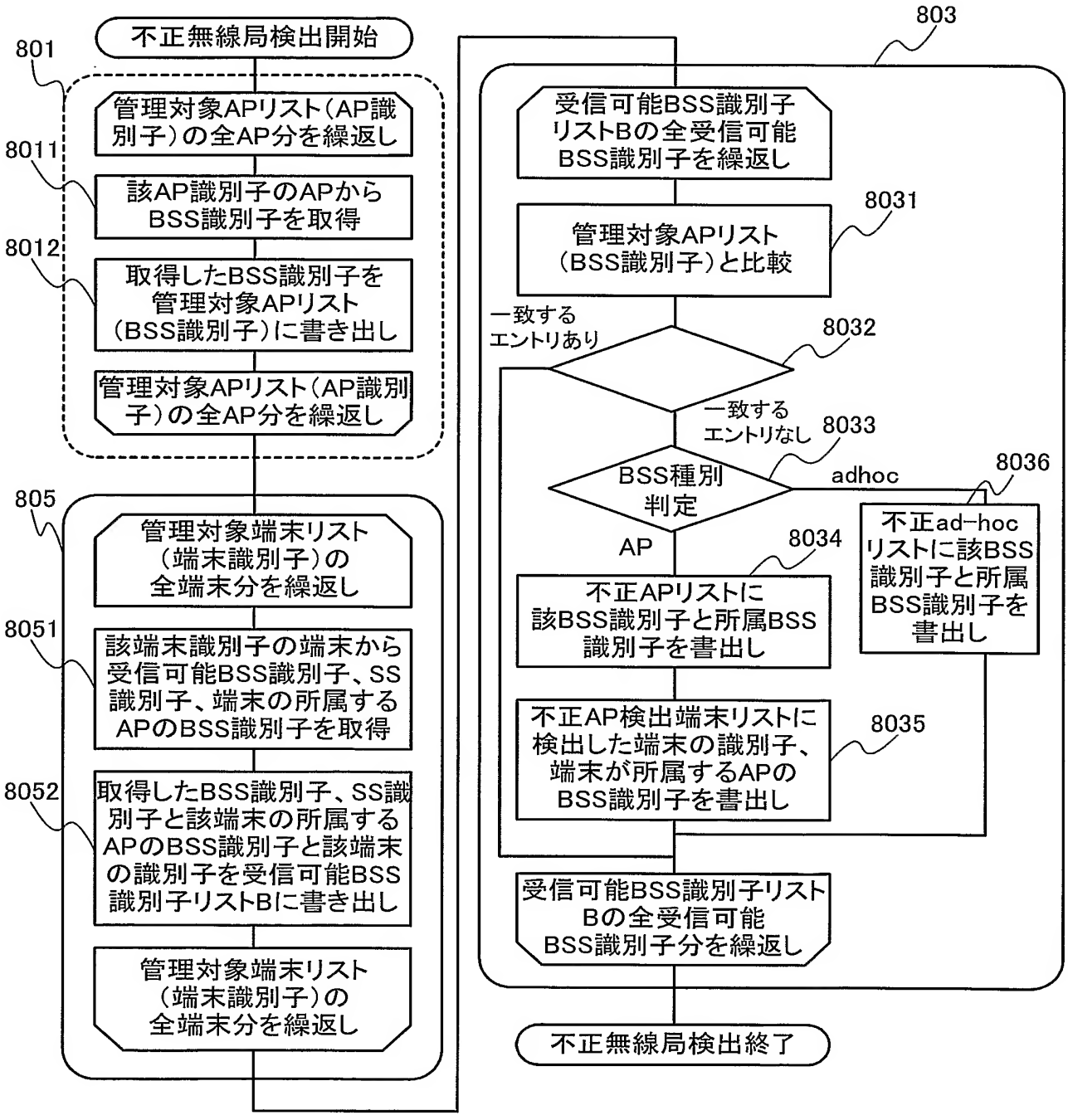
[図18]


運用管理装置
100
101
管理対象APリスト (BSS識別子)
102
受信可能BSS 識別子リストB
103
不正APリスト
104
不正ad-hoc リスト
105
不正AP利用 端末リスト
112
不正AP検出 端末リスト
113
監視処理 実行部
114
フレーム送信元 識別子リストB
106
管理対象APリスト (AP識別子)
管理対象端末 リスト (端末識別子)
107
演算処理部
108
AP設置位置 リスト
109
SW設置位置 リスト
110
送受信部
111
SW-A
SW-B
AP-C
AP-B
表示装置
200
201
表示部
202
送受信部
正規アクセスポイントA
300
有線送受信部
301
BSS識別子 格納部
302
不正無線局 リスト
303
不正無線局 SSID格納部
309
フィルタリング 識別子格納部
308
無線送受信部
304
◇不正無線局
◇アクセスポイント
●01:23:45:67:89:ab
× 00:aa:bb:cc:dd:ee
○00:aa:bb:cc:dd:ef
●00:11:22:33:44:55
●00:66:77:88:99:aa
◇アドホック
●41:23:45:67:89:ab
●70:11:22:33:44:55
●50:66:77:88:99:aa
正規クライアント端末
400
無線送受信部
401
検索処理実行部
402
受信可能BSS 識別子リストC
407
メッセージ 受信・表示部
405
所属BSSの 識別子保持部
406
不正無線局
500
正規クライアント端末2

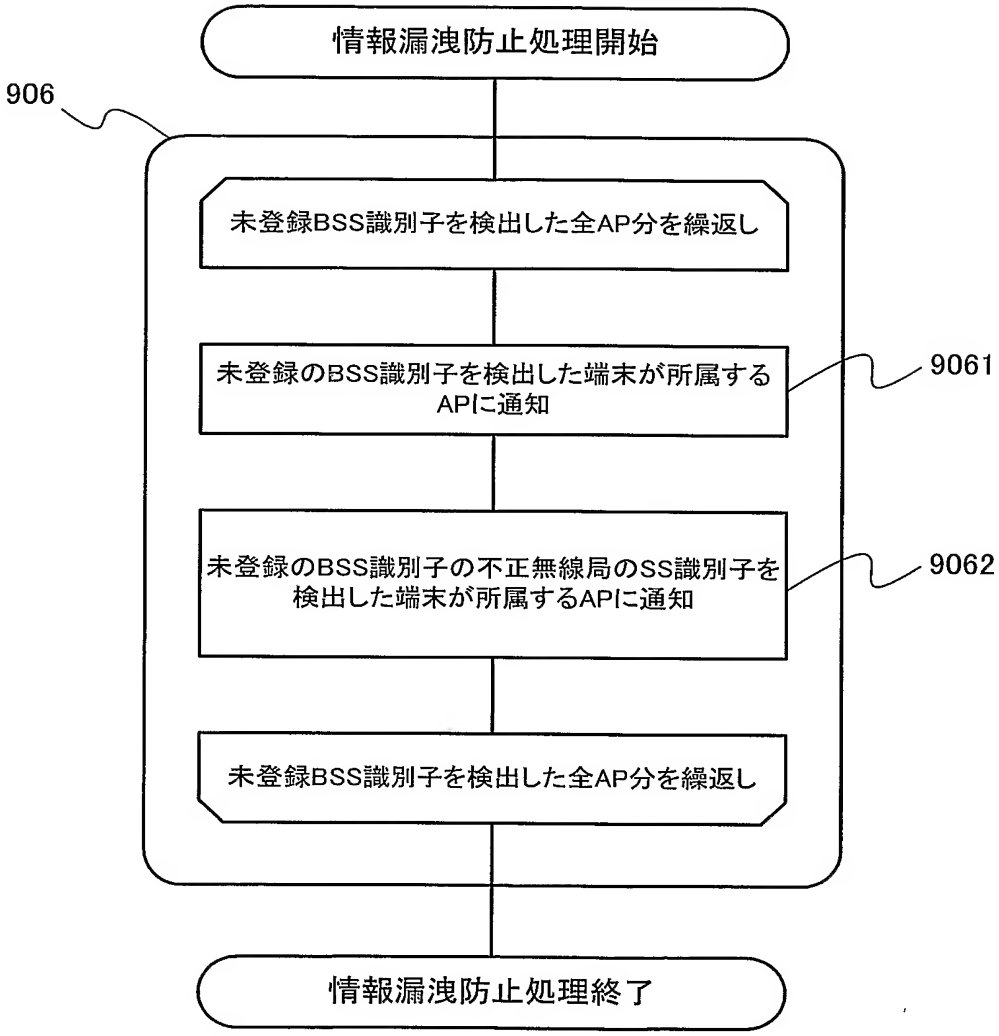
[図19]

端末識別子	所属BSS識別子	受信可能BSS識別子	受信可能SSID
STA1	BSS-1		
STA2	BSS-1		
STA3	BSS-1	R-BSS-1	R-AP
STA4	BSS-4	R-BSS-1	R-AP
		BSS-2	B4-AP

[図20]


不正無線局検出開始
801
管理対象APリスト(AP識別子)の全AP分を繰返し
8011
該AP識別子のAPからBSS識別子を取得
8012
取得したBSS識別子を管理対象APリスト(BSS識別子)に書き出し
管理対象APリスト(AP識別子)の全AP分を繰返し
805
管理対象端末リスト(端末識別子)の全端末分を繰返し
8051
該端末識別子の端末から受信可能BSS識別子、SS識別子、端末の所属するAPのBSS識別子を取得
8052
取得したBSS識別子、SS識別子と該端末の所属するAPのBSS識別子と該端末の識別子を受信可能BSS識別子リストBに書き出し
管理対象端末リスト(端末識別子)の全端末分を繰返し
803
受信可能BSS識別子リストBの全受信可能BSS識別子を繰返し
8031
管理対象APリスト(BSS識別子)と比較
一致するエントリあり
8032
一致するエントリなし
8033
BSS種別判定
adhoc
8036
不正ad-hocリストに該BSS識別子と所属BSS識別子を書出し
AP
8034
不正APリストに該BSS識別子と所属BSS識別子を書出し
不正AP検出端末リストに検出した端末の識別子、端末が所属するAPのBSS識別子を書出し
8035
受信可能BSS識別子リストBの全受信可能BSS識別子分を繰返し
不正無線局検出終了

[図21]


情報漏洩防止処理開始
906
未登録BSS識別子を検出した全AP分を繰返し
未登録のBSS識別子を検出した端末が所属するAPに通知
9061
未登録のBSS識別子の不正無線局のSS識別子を検出した端末が所属するAPに通知
9062
未登録BSS識別子を検出した全AP分を繰返し
情報漏洩防止処理終了

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/002494

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L12/28, H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L12/28, H04Q7/38

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Toroku Jitsuyo Shinan Koho	1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	JP 2003-198571 A (International Business Machines Corp.), 11 July, 2003 (11.07.03), Par. Nos. [0021] to [0033], [0039] & US 2003/0117985 A1	1-3,7,9, 13-15,19,21, 28,30,32,33, 35 4-6,8,10-12, 16-18,20, 22-27,29,31, 34
A	JP 2003-110570 A (Masupuro Denko Kabushiki Kaisha), 11 April, 2003 (11.04.03), Par. Nos. [0048], [0058] to [0060] (Family: none)	10,11,22,23

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 April, 2005 (07.04.05)	26 April, 2005 (26.04.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００５／００２４９４

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.[7]　H04L12/28, H04Q7/38

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.[7]　H04L12/28, H04Q7/38

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００５年
日本国実用新案登録公報	１９９６－２００５年
日本国登録実用新案公報	１９９４－２００５年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	ＪＰ　２００３－１９８５７１　Ａ（インターナショナル・ビジネス・マシーンズ・コーポレーション）２００３．０７．１１，【００２１】－【００３３】，【００３９】& US 2003/0117985 A1	1-3, 7, 9, 13-15, 19, 21, 28, 30, 32, 33, 35
A		4-6, 8, 10-12, 16-18, 20, 22-27, 29, 31, 34

☑ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 ０７．０４．２００５	国際調査報告の発送日 26. 4. 2005
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　5X　9299 中木　努 電話番号　０３－３５８１－１１０１　内線　３５５６

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００５／００２４９４

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	ＪＰ　２００３－１１０５７０　Ａ（マスプロ電工株式会社）２００３．０４．１１，【００４８】，【００５８】－【００６０】（ファミリーなし）	10, 11, 22, 23